SIR THOMAS RICH'S
Information and Communication Technology Policy

Date reviewed: November 2022
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 and Aims

ICT plays a vital role in a successful school. It supports teachers in delivering interesting and effective lessons, offers pupils enriched learning experiences promoting initiative and independent learning; it is also plays an integral role in running the School effectively and in this capacity is used by staff, trustees and volunteers. 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 the ICT resources and facilities used also pose risks to data protection, online safety and safeguarding. This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Ensure that members of the school 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
- Support the school's policies on data protection and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems This policy covers all users of our school's ICT facilities, including trustees, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under the School's *Behaviour and Discipline Policy* or the School's *Staff Code of Conduct* and *Staff Disciplinary Procedure*.

2. Relevant Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2022
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

3. ICT Facilities and Responsibilities

In addition to computers in the Learning Resource Centre and other dedicated study areas, there are computer available for student (and staff) use in four dedicated computer rooms along with additional computers in specialist rooms for Design and Technology and Computers in Music teaching rooms. All classrooms have a projector and many also have an interactive whiteboard.
The amount of printing carried out by pupils is constantly monitored and prints are only released at shared printers when users are physically present (by use of fingerprint recognition for pupils and ID cards for staff).

The School has wireless internet connection (Wi-Fi), giving laptop users access to login via Remote Access. The content is filtered as for a regular school PC. 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.

The School uses both SharePoint and Teams to allow collaborative and remote learning; other shared resources can be accessed both in school and from home through remote access. These systems are used to provide information and support for students such as past examination papers and other resources. The School also uses Satchel One (previously called Show My Homework) for the setting of work to be completed at home. (*See Learning and Teaching Policy, Curriculum Policy*).

3.1 Responsibilities

The **Senior Leadership 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.

The **Network Manager** is 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 use of individual passwords.
- Staff access to the School's networks requires two-factor authentication.
- 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.

(some of these tasks may be delegated to other members of the ICT team).

Teachers and support 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. (see appendices)

Pupils are responsible for working in compliance with the ICT Acceptable Use Policy for pupils (see appendices)

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 (see appendices)

4. The Provision of ICT and Computing Within the Curriculum

Most pupils 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 an optional subject at GCSE and A-Level.

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 using a text-based language. Year 9 students extend these skills further to include more complex topics and traditional programming, as well as covering Social, Ethical and Legal issues in Computing. The Key Stage 3 Computing courses set out to develop the skills that students will need to allow them to code programmes and understand how programmes work, cover the skills pupils need to be responsible digital citizens, and include relevant sections of the KS3 National Curriculum.

4.1 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 assemblies. Staff are trained on e-safety issues and it is explicitly included in relevant curricula (e.g. Computing, PSHE) but is also embedded in the use of ICT throughout all curriculum areas. For further information contact Mr P. Johnson, Head of Computing pwj@strs.org.uk and refer to section 17 of the School's *Child Protection and Safeguarding Policy*

5. Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary actions (see section 5.2 below). There are separate acceptable use policies for different members of the school community which users must follow as appropriate; these are contained as appendices to this policy.

Unacceptable use of the school's ICT facilities includes:

- Using the School's ICT facilities to breach intellectual property rights or copyright
- Using the School's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the School's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the School, or risks bringing the School into disrepute
- Sharing confidential information about the School, its pupils, or other members of the school community
- Connecting any device to the School's ICT network without approval from authorised personnel or in accordance with the School's *Mobile Phone and Personal Device Policy* policy (see Appendix 1).
- Setting up any software, applications or web services on the School's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the School's ICT facilities including sharing lo in details or leaving equipment unattended while logged in
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission

by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the School's filtering mechanisms

This is not an exhaustive list. The School reserves the right to amend this list at any time. The Senior Leadership Team or Network Manager will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

5.1 Exceptions from unacceptable use
Where the use of School ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headmaster's discretion. Request should initially be made to the Network Manager, Mr Matthew Hopton, mph@strs.org.uk

5.2 Sanctions
Any user who engages in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies. These sanctions may include restrictions on access to School ICT facilities. Criminal acts will be referred to the appropriate authorities. Other sanctions for pupils are as set out in the *Behaviour and Discipline Policy*; staff, sanctions will be in accordance with the *Staff Disciplinary Procedure*

6. Staff Use of ICT

The School's Network Manager manages access to the school's ICT facilities and materials for school staff. This includes use of computers, tablets and other devices as well as access permissions for certain programmes or files.

6.1 Staff Access to ICT facilities
Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities. They will be issued with a smart ID card required to access some printing facilities and two-factor authentication (either as an app or a hardware token). Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Network Manager – currently Mr Matthew Hopton mph@strs.org.uk

6.2 Staff Use of Email
The School provides each member of staff with an email address. This email account should be used for work purposes only and all work-related business should be conducted using the email address the School has provided. Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract and may also put the reputation of the school at risk. Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
Staff must take extra care when sending sensitive or confidential information by email. Any emails sent to external contacts with attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. The School makes use of Egress or functionality within Outlook for encryption and further details can be obtained from the ICT team.
If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
If staff send an email in error which contains the personal information of another person, they must inform the *Data Protection Lead* (currently Mr David Dempsey) immediately and follow our data breach procedure.

6.2 Staff Use of Phones
Use of School phones for personal matters should be in accordance with the Personal Use section below.
The School has a Voicemail facility and staff have the choice of accessing the Voicemail service via a School phone or having voicemails sent to their School email.

Staff are permitted to use their personal devices (such as mobile phones or tablets) in line with Mobile Phone and Personal Devices Policy (see appendices)

6.3 Personal Use

Staff are permitted to occasionally use school ICT facilities (including the school phone system) for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Senior Management Team or Network Manger may withdraw permission for it at any time or restrict access at their discretion. Personal use is permitted provided that such use:

- Does not take place during contact time (i.e. in lessons)
- Does not constitute 'unacceptable use', as defined in section 5
- Does not hinder staff from carrying out their job effectively, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos). Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them. Staff should take care to follow the school's guidelines on social media (see appendices) and use of email (see section 6.2) to protect themselves online and avoid compromising their professional integrity.

6.4 Loan of School Devices

The School may facilitate either short-term or long-term loans of equipment to staff. Short-term loans are usually reserved for use within School. If equipment is loaned to a member of staff he/she is responsible for its safekeeping and appropriate use.

For long-term loans, equipment 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 equipment is covered by any licence requirements.

6.5 Remote Access

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
- 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
- that they follow the Staff Acceptable Use policy while connected to Remote Access

6.6 Personal Backups

Staff are discouraged from bringing storage devices in from home and connecting these to the network: there is a risk of inadvertently bringing in malware this way. It is preferable to use Remote Access to work on data or resources for School since all our normal security will be applied/available.

If staff take a personal back up of their resources this must not include personal staff or pupil data.

If staff do use a device for backing up their personal files, they are advised to use a new backup device each time.

If staff wish to restore a backup of data or resources from a personal storage device they should bring this to the ICT office so that ICT staff can confirm the device and files contained on it are clean before the information is restored.

7. Pupils' Use of ICT

The School's Network Manager manages access to the school's ICT facilities and materials for pupils. If issues cannot be dealt with by teaching staff, pupils may seek support from the ICT team.

7.1 Pupil Access to ICT facilities

Pupils may use the ICT suites in C1 to C3 before school from 7.45 am, at break/lunchtime and after school until 4.15pm. Facilities in the LRC can also be used by pupils at these times with computers on the mezzanine floor restricted to pupils in Years 12 and 13. These facilities are monitored remotely by CCTV. ICT equipment in other areas of the school and at other times should only be used under direct staff supervision.

Pupil can also use Remote Access to access the School network from any device:
https://strschool.co.uk/network/remoteaccess

7.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.
The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

7.3 Unacceptable use of ICT and the internet outside School

The school will sanction pupils, in line with the Behaviour and Discipline Policy if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Further details of sanctions are detailed in the *Behaviour and Discipline policy*. Further details of the School's procedures for tackling bullying (which includes cyber-bullying) are included in the *Anti-Bullying policy*.

8. Parents and Visitors' use of ICT

Parents and visitors do not have access to the school's ICT facilities as a matter of course. However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Headmaster's discretion. Likewise, visitors on School business may be granted access. Where parents or visitors are granted access in this way, they must abide by this policy as it applies to staff including the Acceptable Use Policy for staff or pupils, as appropriate. The Network Manager will make the necessary arrangements.

8.1 Communicating with or about the school online

The School believes it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online. Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

8.2 Parent Gateway

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. It also allows parents to update the information held by the School and update any permissions given. If the child's parents live at different addresses, both parents will be offered the service, providing the parent who does not live at the child's registered home has *parental responsibility*. Any reason to withhold access must be supported by appropriate evidence. e.g. court order (note that parents not living at the child's registered address are not able to view or edit the full details of other contacts). Through Parent Gateway, parents also have access to the School SharePoint.

8.3 Other systems

The School may offer parents access to other web-based systems that it is currently using to facilitate its aciviities. For example, parents will be routinely offered accounts for Satchel One (homework); SCOPAY (online payments) and EVOLVE (school trips).

9. Data Security

The School takes its duty to keep data secure very seriously. All users must have regard to the importance of keeping data secure and minimise the risk of loss.

9.1 Passwords

Access by pupils and staff to all types of data held on the School network is only permitted through the controlled issue of passwords and in the cases of staff, who have enhanced access to the system, two-factor authentication. All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked. Password security is covered for students at the start of the Year 7 Computing course and is referred to or revisited in subsequent years. Staff are required to undertake ongoing training on cyber-security.

9.2 Physical Security and Backup

All servers are sited in locked rooms. Pupil records are kept on SIMS. A data backup procedure is implemented: live data is replicated to an on-site backup server every 15 minutes, and an off-site server within 24 hours. The ICT department can use "shadow copies" to retrieve point-in-time file data for up to 30 days from 7am, 12pm or 5pm and snapshots to retrieve point-in-time application data for varying periods depending on the application. Restoration is possible for some parts of the network up to a maximum of 90 days. An 'air-gapped' backup is also performed to help guard against ransomware attacks.

9.3 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must be configured in this way.

9.4 Data protection

Users should be particularly vigilant about logging off at the end of a session when personal data has been accessed. Any personal data removed from site should only be done so with authorization and stored on devices that are either encrypted or secured with two-factor authentication. If personal devices are used (e.g. to store information for an educational visit) this data should be deleted as soon as no longer required for School purposes. All personal data must be processed and stored in line with data protection regulations and the school's *Data Protection policy*.

9.5 Access to facilities and materials

All users of the School's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the Network Manager. Users should not access, or attempt to access, systems, files or devices to which they have not been granted access and alert the Network Manager immediately if they believe that their access is not in accordance with that required by their role.
Users should always log out of systems (or, for staff, lock their equipment) when they are not attended to avoid any unauthorised access. Equipment and systems should always be logged out of at the end of each working day. Peripherals such as projectors should be turned off but computers left on to allow for scheduled updates.

10. Internet Access

The school wireless internet connection is secured and filtered. Staff, pupils and visitors are given appropriate levels of filtering through separately controlled connections to the network. Any inappropriate sites that are not adequately filtered should be reported immediately to the ICT team.

Appendix 1

Mobile Phone and Personal Device Policy

1. Introduction

At Sir Thomas Rich's School, we recognise that mobile phones, including smart phones, and other portable devices are an important part of everyday life for our pupils, parents and staff, as well as the wider school community.

Our policy aims to:

- Promote, and set an example for, safe and responsible phone use
- Set clear guidelines for the use of mobile phones and other personal device for pupils, staff, parents and volunteers
- Support the school's other policies, especially those related to child protection and behaviour

This policy also aims to address some of the challenges posed by mobile phones in school, such as risks to child protection, data protection issues, potential for lesson disruption and the risk of theft, loss or damage.

2. Use of mobile phones and personal devices by staff

Staff and other adults associated with the school may bring personal mobile phones or other personal devices (such as tablets or laptops) to School. Teaching staff are not usually permitted to make or receive calls, or send texts during contact time.

There may be circumstances in which it is appropriate for a member of staff to have use of their phone during contact time (for instance in the case of acutely ill dependents or family members) and the Headmaster will decide on a case-by-basis whether to allow for special arrangements.

2.1 Data protection

Staff must ensure use their personal mobile phones is in line with the School's *Data Protection policy*.

2.2 Safeguarding

Staff must refrain from giving their personal contact details to parents or pupils, including connecting through social media and messaging apps.

Care should be taken if using mobile phones to take photographs or recordings which may include pupils; in most circumstances this can be avoided by using school equipment. If a personal mobile device is used, it should be done in accordance with section 2.3 below.

2.3 Using personal mobiles for work purposes

Staff may plan to use their personal device for interactive classroom apps where these have clear educational benefit and as allowed by their Head of Department. Access to other services, such as CPOMS or two-factor authentication for network access, may be facilitated by use of a member of staff's mobile phone.

If it is necessary to take photos or recordings as part of a lesson/school trip/activity, staff should take care with the use of personal mobile phones and, if possible, use school equipment as an alternative. If personal devices are used, they should only be used in contexts where pupils may reasonably expect to be photographed e.g. public sporting events or performances, public areas during offsite visits, whole class teaching activities. In such circumstances, photographs should be transferred to school servers as soon as is feasibly possible and then must be deleted from the personal device and cloud services.

In some other circumstances, it may be appropriate for staff to use personal mobile phones for other work purposes. Such circumstances may include, but are not limited to emergency evacuations; supervising off-site trips and supervising residential visits.

In all circumstances, staff will: use their mobile phones in an appropriate and professional manner, in line with our Staff Code of Conduct and the ICT Policy.

2.4 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.

2.5 Sanctions

Staff that fail to adhere to this policy may face disciplinary action. See the school's staff disciplinary policy for more information: Staff Disciplinary Procedure

3. Use of mobile phones and personal devices by pupils

3,1 Pupil Use of Mobile Phones

Pupils may bring mobiles phones to School only in accordance with the School Rules which can be found in the Behaviour and Discipline Policy

3.2 Photography

Pupils should not take photographs or video recordings in School without explicit permission from a member of staff. Any photographs or videos taken with permission should not be uploaded to internet sites or social media unless pupils have been given explicit permission by the Headmaster.

3.3 Pupils Use of Laptops, Tablets and E-Readers

Pupils in the Sixth Form may bring these devices to school for educational use in the Sixth Form Centre. Use of such devices outside of the Sixth Form Centre or by pupils in Years 7-11 will only be allowed if permission has been sought in advance and given by a member of staff (this may include permission given for SEND reasons). Devices should be used for educational purposes and continued use remains at the discretion of teaching staff.

4. USB Memory Devices

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.

5. Loss, Theft, Damage and Security

Students and Staff who bring their own devices into School do so entirely at their own risk. The School does not take any responsibility for any loss, theft or damage. It is recommended that devices are insured by the individual. Individuals are responsible for the security of their own device and it is recommended that devices are not lent to others.

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 100 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.

Appendix 3

Social Media guidance for staff

1. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
2. Be careful about tagging other staff members in images or posts
3. Don't share anything publicly that you wouldn't be just as happy showing your pupils
4. Don't use social media sites during school contact time
5. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
6. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
7. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
8. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)
9. While some people advocate changing your display name (e.g. to first name and middle name) you should consider this carefully as it can cause problems with proving ownership of your social media account e.g. Facebook.

10. Check your privacy settings:

- Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your old posts and photos
- The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster
- Google your name to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't search for you by name
- Remember that some information is always public; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

a pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team about what's happening

a parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
  - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

you're being harassed on social media, or somebody is spreading something offensive about you

- Do not retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 4

ICT Acceptable Use Agreement 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 as part of a supervised activity
- 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 have 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.

Appendix 5

ICT Acceptable Use Policy for Staff Members, Governors, Volunteers and Visitors

When using Sir Thomas Rich's ICT facilities and accessing the internet in school, or outside school on a work device, users will abide by the following:

- No user may access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- No user may use the ICT facilities in any way which could harm the school's reputation
- Users must not use any improper language when communicating online, including in emails or other messaging services
- No user may use unauthorised software, or connect unauthorised hardware or devices to the school's network
- All use of the system must be under each user's own username and password. Passwords should not be revealed to anyone. If a user believes someone has obtained their password, they must contact a member of the ICT department. Sanctions exist for any user disclosing passwords.
- Users must not use the network in any way which would disrupt use of the service by others.
- Users must not attempt to bypass the internet filtering system.
- Users must observe copyright regulations and avoid plagiarism.
- Users must follow School policies on the use of mobile phones and other digital appliances.
- Users may not promote private businesses, unless that business is directly related to the school
- All users must understand that the school will monitor the websites visited and use of the school's ICT facilities and systems.
- All users will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- Users will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs them that they have found any material which might upset, distress or harm them or others, and will also do so if they encounter any such material.
- All users will always use the school's ICT systems and internet responsibly, and ensure that pupils in their care do so too.

Appendix 6

School Social Media Accounts

The School operates four main social media accounts on Facebook, Twitter, Instagram and LinkedIn:

Facebook: www.facebook.com/SirThomasRichsSchool
Twitter: @strsglos
Instagram: www.instagram.com/sirthomasrichs
LinkedIn: https://www.linkedin.com/company/sir-thomas-rich's-school

In addition, the School runs a YouTube channel for promotional and other school films, and there are a number of Twitter and Instagram accounts run by departments.

The ICT Manager and the Marketing, Communications and Events Manager have access to, operate and monitor the four main School social media accounts and YouTube channel.

Staff can post on the School's main social media accounts by posting a news item on the school website, which automatically re-posts to Twitter and Facebook, or by emailing details to the Marketing, Communications and Events Manager (sjv@strs.org.uk)

1. Department, Club and Society Social Media Accounts

Departments, clubs and societies may set up and operate their own Twitter or Instagram accounts.

If a member of staff would like to set-up a Twitter or Instagram account for their department, they must firstly seek permission from the relevant Head of Department. Where a member of staff would like to set-up a Twitter or Instagram account for a club or society that they lead or oversee, they must firstly seek permission from the Deputy Headmaster i/c extra-curricular provision.

If a member of staff would like to set up an account using a social media platform other than Twitter or Instagram, they must seek permission from the relevant Head of Department and a member of the SMT bearing in mind that the main School Facebook page and the Alumni Facebook page should remain as the School's only Facebook accounts.

When setting up the social media account, staff should work in tandem with the Marketing, Communications and Events Manager who will be able to offer guidance.

Passwords should be strong, and should be sent to the ICT Manager (mph@strs.org.uk) to be kept in a digital password safe, in order that all School social media accounts are accessible.

Students must not have password access to, or operate, department social media accounts.

Department, club and society social media accounts should be active and posted to regularly (at least every ten days), or should be deleted.

2. Branding and Presentation

Staff should be aware that all School social media accounts and posts represent the School, and must be consistent with our aims and values.

Department accounts must use the correct version of the School crest, and all other images or video clips should be of good quality and reflect the School's brand and high standards (see the School's brand guidelines in File Exchanges for guidance on usage of the crest, house style, tone and voice). Staff should also contact the Marketing, Communications and Events Manager for advice and guidance on branding and house style.

3. Inappropriate Content and Use

School social media accounts must not be used to post, share or spread inappropriate content, or to take part in any activities that may bring the School into disrepute.

When sharing a third-party news article, blog post or other piece of content on School social media accounts, staff must always review the content and source thoroughly before posting.

Staff must not post or share confidential or sensitive information on social media.

(Also see Appendix 5 of the ICT policy and Staff Code of Conduct)

4. Photo Permissions for Students

Photo permissions must be checked for all students appearing in pictures posted on the School website, and on School, department, club or society social media accounts. Staff must not post pictures of students for whom we do not have permission to do so.

Permissions can be checked in SIMS, or by pressing CTRL+SHIFT+F keys or staff can request a report from the Student Data Administrator (sdb@strs.org.uk).

5. Student-run Social Media Accounts

Students running a social media account associated with the School, for example a School society or club, must give password access to their supervising member of staff, who must also pass the details to the ICT Manager. Before the student leaves, control must be handed to another person. This includes changing the email address and phone number associated with that account. As stated above, students must not have password access to, or operate, department social media accounts.

The supervising member of staff is responsible for regularly monitoring the account, ensuring that branding and use of the school crest is correct. The member of staff should ensure that both they and the student(s) running the social media account adhere to the acceptable use policies (see Appendix 4 and Appendix 5 of the ICT policy).