ICT & eSafety Policy

St Laurence School Academy Trust

Date of last review:	May 2019	**Review period:**	2 years
Date of next review:	May 2021	**Owner:**	DFO / ICT Manager

The need for a policy

All St Laurence School's information communication technology (ICT) facilities and information resources remain the property of St Laurence School and not of particular individuals, teams or departments. By following this policy we will help ensure that ICT facilities are used:

- legally;
- securely;
- without undermining St Laurence School;
- effectively;
- in a spirit of co-operation, trust and consideration for others;
- so as to create an environment in which students can learn and develop and staff can have fulfilling careers, free from harassment and bullying;
- So users can understand and can safely use existing and emerging technologies and understand the benefits and risks of using technology that accesses the internet;
- so that they remain available.

The policy relates to all ICT facilities and services provided by St Laurence School, although special emphasis is placed on email and the internet. All employees, temporary staff, students and visitors and any other users of our IT are expected to adhere to the policy.

Consultation

The policy has been developed through consultation with staff, students and governors. The policy should be considered in conjunction with other relevant policies such as the Child Protection Policy, Code of Conduct for Staff & Volunteers at St Laurence School, Behaviour Policy, Anti-bullying Policy and Dignity at Work Policy. This policy takes into consideration DfE guidance on Preventing and Tackling Bullying (2017) and on Cyberbullying (2014) and also the recommendations of the St Laurence audit of our e-safety curriculum (2017). Due to the rapidly changing world of information technologies, changes to current practice may be made at any time to ensure the safety of all users.

1. eSafety Training and Teaching

The education of students in e-safety is an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

1.1. A planned and up-to-date e-safety programme will be provided as part of the Information and Communication Technology (ICT) and Personal and Social Health Education curriculum, covering both the use of ICT and new technologies both in and outside school. This will include the Acceptable Use Agreement which will be printed in student planners and posted in all ICT rooms and on the school website.

1.2. The e-safety curriculum will include technical aspects of e-safety.

1.3. Key e-safety messages will be reinforced regularly in assemblies / briefings and tutorial/pastoral activities.

1.4. Students will be taught in lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information and the authenticity of the source.

1.5. Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

1.6. Students will be taught about the relevant legislation about e-safety, including laws about image sharing, the Malicious Communications Act 1988 and the Communications Act 2003.

1.7. The school will offer advice and information about e-safety issues in the school newsletter, on the school website and through other literature, as appropriate, in order that parents and other family members can gain a better understanding of these issues.

1.8. All staff will receive regular (at least annual) e-safety training and understand their responsibilities, as outlined in this policy. All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school's E-safety Policy and Acceptable Use Agreements. The designated member of the senior leadership team will co-ordinate advice, guidance and training as required.

2. Roles and Responsibilities

2.1. The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the designated member of the senior leadership team. The Headteacher will ensure that there is a system in place to allow for monitoring, support and protection of those in school who carry out the internal e-safety monitoring role. The Headteacher is responsible for reporting any serious e-safety allegations being made against a member of staff in line with the school staff code of conduct and Local Authority Safeguarding Procedures.

2.2. The designated member of the senior leadership team, with support from the Network Manager and Designated Safeguarding Lead, is responsible for developing the E-safety Policy and procedures; providing training and advice for staff; liaising with the Local Authority and school ICT technical staff; supporting staff in dealing with e-safety incidents. The school will also seek to provide information and awareness to parents and carers through: letters, newsletters, the school web site and parents' evenings. Where breaches of E-Safety occur these will be acted on and recorded in line with the relevant policies affecting staff and/or students.

2.3. Teaching and Support Staff are responsible for ensuring that they have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices.

2.4. The Network Manager is responsible for ensuring that:

2.4.1. The school's ICT infrastructure is secure and is not open to misuse or malicious attack.

2.4.2. The school meets the e-safety technical requirements outlined by Ofsted requirements in the South West Grid for Learning Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.

2.4.3. Users may only access the school's networks through a properly enforced password protection policy. In line with best practice advice by Microsoft, passwords do not expire, however strong passwords are enforced and it is recommended to have different passwords for each individual system.

2.4.4. User's access to network folders and the school management software (SIMS) is appropriate for their role.

2.4.5. He/She keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

2.4.6. The use of the network, remote access, email and externally hosted school E-Systems are regularly monitored in order that any misuse or attempted misuse can be reported to the Assistant Headteacher for investigation.

2.4.7. Monitoring software systems are implemented and updated as appropriate.

2.5. Students are responsible for using the school ICT systems in accordance with the Acceptable Use Agreement which will be introduced to them as part of the tutorial program and which they have to agree to before being given access to school system.

2.6. Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way, both in and out of school. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through newsletters, the school's website and other methods of communication. Parents and carers will be responsible for: endorsing by signature the student Acceptable Use Agreement in their children's planners.

2.7. Community Users who access school ICT systems/website/ as part of the Extended School provision will be expected to agree to the Acceptable Use Agreement before being provided access to school systems.

3. Security guidance for users:

3.1. As a user of St Laurence School's equipment and services, you are responsible for your activity.

3.2. Do not disclose personal system passwords or other security details to other employees, students, parents/carers or external agents, and do not use anyone else's log-in; this compromises the security of St Laurence School. If someone else gets to know your password, ensure that you change it or get the IT Department to help you.

3.3. If you intend to leave your PC or workstation unattended for any reason, you should lock the screen to prevent unauthorized access. If you fail to do this, you will be responsible for any misuse of it while you are away. Logging off is especially important where members of the public and students have access to the screen in your absence.

3.4. Any pen drives or other storage devices on St Laurence School's network are encrypted, users will not be able to write any data to the device until the encryption is applied. Please note this applies to staff only as students do not have access to any sensitive information.

3.5. Do not attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you do not have access to information or resources you feel you need, contact the IT Department.

3.6. Users of the system are expected to familiarize themselves with the school's guidance on recognising and dealing with spam and phishing emails.

4. Use of Email

4.1. Use email in preference to paper to reach people quickly (saving time on photocopying / Distribution) and to help reduce paper use.

4.2. Use the phone for urgent messages (email is a good backup in such instances). Use of email by employees, temporary staff, students and visitors of St Laurence School is permitted and encouraged where such use supports the goals and objectives of St Laurence School.

4.3. However, St Laurence School has a policy for the use of email whereby employees and volunteers must ensure that they:

4.3.1. comply with current legislation;

4.3.2. use email in an acceptable way;

4.3.3. Do not create unnecessary business risk to St Laurence School by their misuse of the internet.

4.4. Unacceptable behavior:

4.4.1. Sending confidential information to external locations without appropriate safeguards in place.

4.4.2. Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.

4.4.3. Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist, homophobic or racist, or might be considered as harassment or bullying.

4.4.4. Using copyrighted information in a way that violates the copyright.

4.4.5. Breaking into St Laurence School's or another organisation's system, or unauthorised use of a password / mailbox.

4.4.6. Broadcasting personal views on social, political, religious or other non-business related matters.

4.4.7. Transmitting unsolicited commercial or advertising material.

4.4.8. Undertaking deliberate activities that waste employee's effort or networked resources.

4.4.9. Deliberately or recklessly introducing any form of computer virus or malware into the corporate network.

4.5. Confidentiality

4.5.1. Always exercise caution when committing confidential information to email since the confidentiality of such material cannot be guaranteed. St Laurence School reserves the right to monitor electronic communications in accordance with applicable laws and policies. The right to monitor communications includes messages sent or received by system users

(employees, temporary staff, students and visitor) within and outside the system as well as deleted messages.

4.5.2. When publishing or transmitting information externally be aware that you are representing St Laurence School and could be seen as speaking on St Laurence School's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager;

4.5.3. Check your inbox at regular intervals during the working day. Keep your inbox fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical);

4.5.4. Keep electronic files of electronic correspondence, only retaining what you need to. Do not print it off and keep paper files unless absolutely necessary.

4.5.5. Treat others with respect and in a way in which you would expect to be treated yourself (e.g. do not send unconstructive feedback, argue, or invite colleagues to make public their displeasure at the actions / decisions of a colleague).

4.5.6. Do not forward emails warning about viruses (they are invariably hoaxes and the IT Department will probably already be aware of genuine viruses – if in doubt, contact them for advice).

4.5.7. Do not open an email unless you have a reasonably good expectation of what it contains, and do not download files unless they are from a trusted source. For example, do open report.doc from a colleague you know but do not open explore.zip sent from an address you have never heard of, however tempting. Alert IT Support if you are sent anything like this unexpectedly; this is one of the most effective means of St Laurence School against email virus attacks.

4.5.8. All school business communications needs to be via the schools email system rather than a personal email account. Similarly, personal communications relating to employee's private lives should not use the school account. Governors and Members must ensure that a personal, unshared email account is used for school communications.

4.5.9. In line with the Code of Conduct for Staff & Volunteers, staff should only accept emails from students from the students' School email accounts and where students contact staff by using private email accounts, staff should reply to the students' School email accounts.

4.5.10. In line with the Code of Conduct for Staff & Volunteers, staff should not give personal landline/mobile numbers to students or parents/carers except under exceptional circumstances, e.g. an emergency when no school phones are available.

4.5.11. In line with the Code of Conduct for Staff & Volunteers, staff must not accept "friend" requests on social media from students, present or past, and students must not be part of a member of staff's social networking group.

4.5.12. Staff and students must not respond or retaliate to cyber-bullying incidents. They should report these to, and seek help from, a member of the senior leadership team.

4.6. Email signatures

4.6.1. Keep these short and include your name, title, phone / fax number(s) and website address. Please follow the style provided by St Laurence School.

5. Use of the Internet

The school will be responsible for ensuring that the school infrastructure is as secured against physical attacks, accidental damage, malicious software as is reasonably possible and that this policy is fully implemented. Use of a firewall, antivirus/antimalware software, and physical restriction to critical infrastructure components is mandated. School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined by Ofsted requirements and Acceptable Use Agreement and any relevant Local Authority E-Safety Policy. There will be annual reviews and audits of the safety and security of school ICT systems.

5.1. The school will maintain and support the managed filtering and Firewall service including the use of group based filtering, access and reporting. All internet access is logged against the user's network username.

5.2. Use of the Internet by employees, temporary staff, students and visitors is permitted and encouraged where such use supports the goals and objectives of the school.

5.3. However, when using the Internet, employees, temporary staff, students and visitors must ensure that they:

5.3.1. Comply with current legislation;

5.3.2. Use the internet in an acceptable way;

5.3.3. Do not create unnecessary business risk to the organisation by their misuse of the internet.

5.4. Unacceptable behavior.

5.4.1. In particular the following is deemed unacceptable use or behaviour by employees, temporary staff, students and visitors (this list is non-exhaustive):

5.4.1.1. Using the computer to perpetrate any form of fraud, or software, film or music piracy;

5.4.1.2. Using the internet to send offensive or harassing material to other users;

5.4.1.3. Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;

5.4.1.4. Hacking into unauthorised areas;

5.4.1.5. Creating or transmitting defamatory material;

5.4.1.6. Undertaking deliberate activities that waste employees effort or networked resources;

5.4.1.7. Deliberately or recklessly introducing any form of computer virus into St Laurence School's network.

5.4.1.8. Visiting internet sites that contain obscene, hateful, pornographic or other illegal material;

5.5. Chat rooms / instant messaging (applicable to Staff only)

5.5.1. The use of chat rooms and instant messaging is permitted for business use only. This use must have been agreed with [your line manager].

5.6. Obscenities / pornography

5.6.1. Do not write, publish, look for, bookmark, access or download material that might be regarded as pornographic, obscene, hateful, racist, sexist, homophobic or might be considered as harassment or bullying.

5.7. Copyright

5.7.1. Take care to use software legally and in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

5.7.2. Be aware of copyright law when using content you have found on other organisations' websites. The law is the same as it is for printed materials.

6. Use of Digital Images and Video

6.1. When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.

6.2. Staff are allowed to take digital/video images to support educational aims, but must follow school regulations concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. Personal equipment of staff should not be used for such purposes.

6.3. Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

6.4. Students must not take, use, share, publish or distribute images of others without their permission.

6.5. Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

6.6. Students' full names will not be used anywhere on a website or blog in association with photographs.

6.7. Parents/carers are asked annually if they wish to withdraw the right to photographs of their children being published, for example on the school website.

6.8. Students' work can only be published with the permission of the student.

7. Software

7.1. Software must be purchased with a full license appropriate for the number of computers it is going to be installed on. Prior approval for any installation of software must be sought from IT/the Head Teacher before attempting to install third party software onto the computer.

7.2. Trial software will not be installed on multiple network computers.

7.3. Software licenses and media should be held by the IT department after purchasing.

7.4. There should be a valid educational reason why a piece of software is going to be installed on the network.

7.5. An annual review by the IT Department will take place of the software installed on the network.

8. Confidentiality

8.1. If you are dealing with personal, sensitive and / or confidential information, then you must ensure that extra care is taken to protect the information.

8.2. If sending personal, sensitive and / or confidential information via email, then the following protocols should be used. If there is any doubt as to the information being sent or the appropriate level of protection required, please check with the IT Department.

8.2.1. Personal, sensitive and / or confidential information should be contained in an attachment;

8.2.2. In appropriate cases the attachment should be encrypted, and / or password protected;

8.2.3. Any password or key must be sent separately;

8.2.4. Before sending the email, verify the recipient by checking the address, and if appropriate,

telephoning the recipient to check and inform them that the email will be sent;

8.2.5. Do not refer to the information in the subject of the email.

9. St Laurence School's network

9.1. Keep master copies of important data on St Laurence School's network server and not solely on your PC's local C: Drive or portable disks. Not storing data on St Laurence School's network server means it will not be backed up and is therefore at risk.

9.2. Ask for advice from the IT Department if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disk space very quickly and can bring the network to a standstill.

9.3. Be considerate about storing personal files on St Laurence School's network. Files of this type may be deleted after investigation as to their purpose from the IT Department.

9.4. Do not copy files that are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disk space unnecessarily.

9.5. Your departmental folder on the shared network drives are the responsibility of the department w.r.t deleting unneeded files and general housekeeping.

9.6. Do not make unnecessary copies of data.

10. Removable Media

10.1.1. Always consider if an alternative solution already exists;

10.1.2. Only use recommended removable media;

10.1.3. Encrypt and password protect;

10.1.4. Store all removable media securely;

10.1.5. Removable media must be disposed of securely.

11. Personal use of ICT facilities

11.1. Social media

For the purposes of this policy, social media websites are web-based and mobile technologies which allow parties to communicate instantly with each other or to share data in a public forum. They include websites such as Facebook, Twitter, Google+ and LinkedIn. They also cover blogs and image sharing websites such as YouTube and Flickr. This is not an exhaustive list and you should be aware that this is a constantly changing area.

11.1.1. Use of Social Media at work

11.1.1.1. Employees and volunteers are permitted to make reasonable and appropriate use of social media websites from St Laurence School's IT equipment. You should ensure that usage is not excessive and does not interfere with work duties. Use should be restricted to your non-working hours, unless this forms part of your work responsibilities.

11.1.1.2. Access to particular social media websites may be withdrawn in the case of misuse.

11.1.1.3. Inappropriate comments on social media websites can cause damage to the reputation of the organisation if a person is recognised as being an employee, temporary staff, students and visitor. It is, therefore, imperative that you are respectful of the organisation's service as a whole including parent/carers, colleagues, partners and competitors.

11.1.1.4. Employees, temporary staff, students and visitor should not give the impression that

they are representing, giving opinions or otherwise making statements on behalf of St Laurence School unless appropriately authorised to do so. Personal opinions must be acknowledged as such, and should not be represented in any way that might make them appear to be those of the organisation. Where appropriate, an explicit disclaimer should be included, for example: 'These statements and opinions are my own and not those of St Laurence School.

11.1.1.5. Any communications that employees, temporary staff, students and visitor make in a personal capacity must not:

11.1.1.5.1. bring St Laurence School into disrepute, for example by criticising parent/carers, colleagues or partner organisations;

11.1.1.5.2. breach the St Laurence School's policy on student/parent/carer confidentiality or any other relevant policy;

11.1.1.5.3. breach copyright, for example by using someone else's images or written content without permission;

11.1.1.5.4. do anything which might be viewed as discriminatory against, or harassment towards, any individual, for example, by making offensive or derogatory comments relating to: age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation;

11.1.1.5.5. use social media to bully another individual;

11.1.1.5.6. post images that are discriminatory or offensive (or links to such content).

11.1.2. X maintains the right to monitor usage where there is suspicion of improper use.

11.2. Other personal use

11.2.1. Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, personal phone calls and browsing the internet) is permitted so long as such use does not:

11.2.1.1. incur specific expenditure for St Laurence School;

11.2.1.2. impact on the performance of your job or role

11.2.1.3. break the law;

11.2.1.4. bring St Laurence School into disrepute;

11.2.1.5. detrimentally affect the network performance by using large amounts of bandwidth (for instance by downloading / streaming of music or videos);

11.2.1.6. impact on the availability of resources needed (physical or network) for business use.

11.2.2. Any information contained within St Laurence School in any form is for use by the employee, temporary staff, students and visitor for the duration of their period of work and should not be used in any way other than for proper business purposes, or transferred into any other format (e.g. loaded onto a memory stick / pen drive), unless necessary for business use, and with prior agreement of the Director of Finance and Operations.

12. Portable and Mobile ICT Equipment

12.1. This section covers items such as laptops, mobile devices and removable data storage devices. Please refer to paragraph 7 of this document when considering storing or transferring personal or sensitive data.

12.2. All activities carried out on St Laurence School's systems and hardware will be monitored in accordance with the general policy.

12.3. Employees, temporary staff, students and visitor must ensure that all data belonging to St Laurence School is stored on St Laurence School's network and not kept solely on a laptop.

12.4. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting your journey.

12.5. Synchronise all locally stored data, including diary entries, with the central organisation

network server on a frequent basis.

12.6. Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

12.7. The installation of any applications or software packages must be authorised by the IT Department, fully licensed and only carried out by the IT Department.

12.8. In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

13. Remote Access

13.1. You are responsible for all activity via your remote access facility.

13.2. Laptops and mobile devices must have appropriate access protection, i.e. passwords and must not be left unattended in public places.

13.3. To prevent unauthorised access to St Laurence School's systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.

13.4. Select PINs that are not easily guessed, e.g. do not use your house or telephone number and do not choose consecutive or repeated numbers.

13.5. Avoid writing down or otherwise recording any network access information where possible. Any information that is written down must be kept in a secure place and disguised so that no other person is able to identify what it is.

13.6. Protect St Laurence School's information and data at all times, including any printed material produced while using the remote access facility. Taking particular care when access is from a non-office environment.

13.7. Users of laptops and mobile devices are advised to check their car and home insurance policies for the level of cover in the event of equipment being stolen or damaged. Appropriate precautions should be taken to minimise risk of theft or damage.

13.8. Care should be taken when working on laptops in public places (e.g. trains) that any employee or parent/carer details are not visible to other people.

14. Electronic monitoring

14.1. You may find that you have access to electronic information about the activity of colleagues. Any such information must not be used by unauthorised individuals to monitor the activity of individual employees in any way (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files, etc.) without their prior knowledge. Exceptions are:

14.1.1. In the case of a specific allegation of misconduct, when the Senior Team can authorise accessing of such information when investigating the allegation;

14.1.2. When the IT Department cannot avoid accessing such information while fixing a problem, but this will only be carried out with the consent of the individual concerned.

15. Online purchasing

15.1. Any users who place and pay for orders online using personal details do so at their own risk and St Laurence School accepts no liability if details are fraudulently obtained whilst the user is using St Laurence School's equipment.

16. Care of equipment

16.1. Do not rearrange the way in which equipment is plugged in (computers, power supplies, phones, network cabling etc.) without first contacting the IT Department.

17. Leaving St Laurence School

17.1. Your school network account and email will be retained until the start of the term following your leaving date, so if you leave at the end of term 2 the account will not be deleted until day 1 of term 3.

17.2. Please note 30 days after leaving your school email is hard deleted by Microsoft, and is then irretrievable.

17.3. Your personal 'My Documents (H:)' files are backed up and kept by IT for 1 year.

17.4. Please remove any personal files from the Curriculum or Administration Folders.

17.5. If you have a loan laptop please return to IT.

17.6. If you have a loan iPad please erase it before returning to IT.

18. Disciplinary measures

The Education Act 2011 amended the power in the Education Act 1996 to provide that, when an electronic device has been seized by a member of staff who has been formally authorised by the Headteacher, that staff member can examine data or files, and delete these, where there is good reason to do so. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone.

If an electronic device that is prohibited by the school rules has been seized and the member of staff has reasonable ground to suspect that it contains evidence in relation to an offence, they must give the device to the police as soon as it is reasonably practicable. Material on the devise that is suspected to be evidence relevant to an offence, or that is a suspected pornographic image of a child or an extreme pornographic image, should not be viewed or deleted prior to giving the device to the police. If a staff member finds material that they do not suspect contains evidence in relation to an offence, they can decide whether it is appropriate to delete or retain the material as evidence of a breach of school discipline.

18.1. Deliberate and serious breach of the policy statements in this section may lead to the St Laurence School taking disciplinary measures in accordance with St Laurence School's disciplinary procedure. St Laurence School accepts that ICT – especially the internet and email system – is a valuable business tool. However, misuse of this facility can have a negative impact upon employees, temporary staff, students and visitor's productivity and the reputation of the organisation.

18.2. In addition, all of St Laurence School's phone, internet and email related resources are provided for business purposes. Therefore, St Laurence School maintains the right to monitor the volume of internet and network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

19. Agreement

All employees, temporary staff, students and visitor who have been granted the right to use the St Laurence School's ICT systems are required to sign this agreement confirming their understanding and acceptance of this policy.

Signed:		**Signed:**	
Manager:		**Employee:**	
Date:		**Date:**	