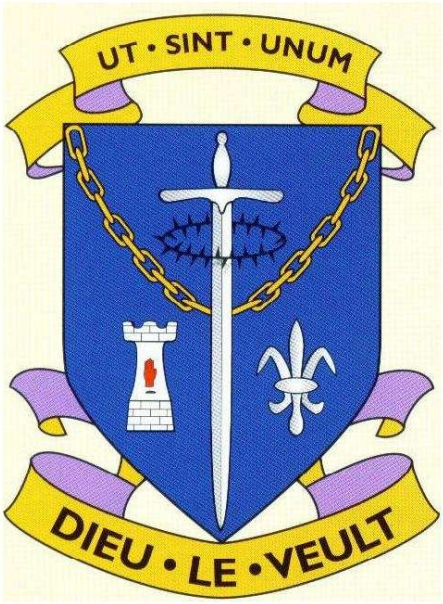
St Louis Grammar School Kilkeel



ICT Acceptable Use Policy

Date of Policy: September 2024

Last Reviewed: September 2023

Reviewed by: Mr T. Brown

Date of Review: September 2025

Contents

1. Introduction

Our E-safety and ICT Acceptable Use Policies (AUP) have been written by the school, in the light of the Department of Education Northern Ireland (DENI) policy, and government guidance. It has been agreed by the staff and Senior Management Team (SLMT) and approved by governors. Pupils have been involved in compiling the rules given out to new year 8 pupils as well as other aspects of the policy.

The policy will next be reviewed on 1/6/2025.

Use of the school's ICT equipment by all staff and pupils must be in accordance with this policy. The SLT will treat any use that infringes this policy very seriously.

2. The Importance of Internet use in Education

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

2.1 Using the Internet to Enhance Learning

The school Internet access will be designed expressly for staff and students use and will include filtering appropriate to the age of pupils provided by C2K. Other visitors may use the school's Internet when it is deemed appropriate.

2.2 How Does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient through websites, online collaboration, and online communication including the use of web cams.
- Access to world-wide educational resources
- Inclusion in Education Network Northern Ireland (ENNI) which connects all NI schools
- Educational and cultural exchanges between students world-wide
- Access to experts in many fields for students and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data with DENI and examination boards

2.3 How Can Internet Use Enhance Learning?

- Pupils will be taught what Internet use is acceptable and given clear objectives for Internet use throughout the Key Stages during IT lessons or through the pastoral programme. This includes: specific lessons, during assemblies, assemblies from outside agencies such as the police, during tutor periods and within the pastoral programme where deemed appropriate.

- Internet access will be planned by staff to enrich and extend learning activities.

- Staff will guide students in on-line activities that will support learning outcomes planned for the students' age and maturity.

- Students will be educated in the effective use of the Internet in research including the skills of knowledge location, retrieval, and evaluation of sources.

2.4 The Need for Pupils to Learn to Evaluate Online Content.

- Pupils must be encouraged to act responsibly when using the Internet and to report any concerns they may have to a member of staff.

- If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the ICT Co-ordinator who will report the URL to ENNI immediately. If inappropriate material has been accessed by the pupil members of the Safeguarding Team will be informed. (**See the guidance flowchart in the e-safety Policy Appendix 2**)

- The school should ensure that the use of Internet derived materials by staff and by pupils complies with all relevant laws (**See Appendix 3 of the e-safety Policy**). The school will inform all staff and pupils of the appropriate way to record relevant URLs, and how to use copyright material legally in school. For students, this is an essential skill that must be evidenced as part of the statutory "Using ICT" assessment at Key Stage 3.

- If staff wish to make available to students a site that is currently unavailable through the schools' filter, they must consult with the Director of ICT and e-learning who will first consider the sites appropriateness for teaching and learning. If deemed appropriate the Director of ICT and e-learning will communicate directly with ENNI.

- If staff wish to gain access to a site for educational purposes that is currently unavailable through the C2K or schools wireless network for use on staff iPads, for example, they must apply first in writing to the Director of ICT and e-learning.

3. The Management of School e-mail.

- Staff may use the school email system to contact pupils individually or in year groups for educational purposes only.

- Staff may use the school email system for education purposes only.

- Pupils may only use approved e-mail accounts on the school system and email must be used for educational purposes only unless a need has been identified for them to use personal email accounts (e.g. UCAS).

- Pupils must immediately tell a teacher if they receive offensive e-mails through their school email account.

- Pupils will be taught to not reveal details of themselves or others in e-mail or other online communication, such as address or telephone number.

- Pupils must only use their school email address to sign up for services and activities approved by the school. However, sixth form students may use a personal email account when registering their details for UCAS.

- E-mail sent to external organisations should be written carefully and, in the case of pupils, authorised by a teacher before sending. The rules of Netiquette must be followed at all times.

- Staff and pupils must be aware that when using school e-mail from home through MySchool that they are still using the school system and treat all communications appropriately.

- All school staff are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the public sector.

- All users should be aware that network administrators from ENNI may review files and communications to maintain system integrity and to ensure that users are using the system responsibly and legally. While normal privacy is respected and protected by password controls, users may not expect files and messages stored on publicly-funded networks to be private. The school also employs the Securus system which allows live monitoring of the use of email and highlights pupils who have used banned words in messages they receive or send. This evidence is retained. Securus is monitored by the VP and the Director of ICT and e-learning on a rotational basis.

- Staff must also be aware that electronic communication is a form of evidence that may be requested by a court of law.

4. The Management of Discussion Forums, Video Conferencing and Chat Rooms.

- Pupils will be allowed to take part in discussion forums that are controlled by staff or other responsible adults within and outside school using the schools GOOGLE CLASSROOM.

- All pupils and staff must agree to the terms and conditions of appropriate usage before using the schools GOOGLE CLASSROOM - these can be seen in GOOGLE CLASSROOM policy and GOOGLE CLASSROOM Code of conduct.

- The use of video conferencing facilities in school will be for approved activities only and all such use by groups of pupils will be monitored continuously by staff members.

- Pupils may also use the schools video conferencing facilities when being taught through video conferencing by another school, or when used as part of an international program, and this will be monitored by a member of staff.

- Unmanaged chat rooms must not be used in school unless they are required for a specific subject and for a specific purpose. When used they will be fully monitored by members of staff. The importance of chat room safety will be emphasised by staff prior to use and through the ICT Key Stage 3 curriculum. Chat rooms will be used for educational purposes only.

- Pupils will be able to make use of supervised chat facilities through the schools GOOGLE CLASSROOM in accordance with the GOOGLE CLASSROOM policy.

5. External Access to Software, User Areas, Google Classroom and Email

- The school will grant pupils and staff access to software, their user areas, the GOOGLE CLASSROOM and email from home using their own ENNI username and password through MySchool.

- Pupils must be made aware of 'best practice' by staff when using external access and in particular how to save work produced at home to their own personal storage area.

- The school is not liable for any loss or damage to pupil or staff files caused unintentionally or by inappropriate or misguided use of the external facilities.

- The school also allows pupils to upload assignments that have been set to be completed electronically either in lessons or through the GOOGLE CLASSROOM. Pupils will be made aware of the importance of keeping copies of any work they have uploaded to the GOOGLE CLASSROOM at home and in their MyDocs. Pupil's use of the GOOGLE CLASSROOM will be in accordance with the GOOGLE CLASSROOM policy and GOOGLE CLASSROOM Code of conduct.

6. External Assessment / Controlled Assessment

- Pupils may use the IT facilities to complete work required for controlled assessment for GCSE under supervision by a teacher. The level of supervision is dictated by the individual controlled assessment requirements.

- Teaching staff must be aware of the requirements for keeping such electronic work secure, controlling access to work outside of lesson times, and the particular rules that apply to internet access when completing controlled assessment within school.

- C2K provide facilities for the creation of exam / controlled assessment accounts which allow the school to control access. If a staff member wishes to create such accounts, the Director of ICT and e-learning must be informed at least two weeks prior to when the accounts are needed.

- Staff must also be aware of the following for any controlled assessments they conduct:

    - Inspections will be conducted each year with a different subject selected. Visits may take place directly at controlled assessments events each year – CCEA will give advanced notice about this.

    - All controlled assessments completed electronically must be safely stored in the students account and students must not have access to the account outside of normal class hours or as dictated by the exam board.

    - If a time limit is set on your controlled assessment keep a log of all timings.

7. The Management of Internet Access

- The school will keep a record of all staff and pupils who are granted Internet access through the ENNI system. The record will be kept up-to-date, for example when a

member of staff may leave or a student's access may be withdrawn for abuse of the system.

- Parents of year 8 pupils will be informed that pupils will be provided Internet access (a copy of the letter is included in Appendix 1).

- Pupils must apply for Internet access individually by agreeing to abide by the Responsible Internet Use statement. Parents will be asked to sign and return a consent form during the year 8 induction in June.

- Pupils must also apply for access to the schools' GOOGLE CLASSROOM by agreeing to abide by the GOOGLE CLASSROOM Code of Conduct (See GOOGLE CLASSROOM Policy).

- Pupils in sixth form may access the Internet wirelessly using their own devices only when they have read and agreed to the Wireless Internet Policy. Their parents must also sign the consent form to acknowledge that they are aware that a pupil is using a personal device in school. Pupils who wish to use their laptops in school without connecting to the schools' Internet must also have the consent form signed. (**See Appendix 3**).

8. Management of Emerging Internet Applications

- The policy on emerging technologies will be reviewed on an annual basis to take account of the risks associated with them.

- Mobile phones will not be used without permission during the school day between the hours of 8:45am and 3:45pm. This includes the use of any mobile technology to access the Internet or World Wide Web through the schools network or the public telecommunications network. (Please refer to the schools positive discipline policy)

- Portable storage devices such as MP3 players, PDAs, Camera phones, or any other device that is capable of storing and displaying images, video or sound recordings, should not be used between the hours stated above. However, the use of portable storage devices for transporting files between school and home is permitted under certain circumstances. (Please refer to the schools positive discipline policy)

- Pupils and staff are allowed to use portable storage devices such as flash drives or memory sticks / USB pens. However the owner must check these prior to use for viruses. If in doubt consult a member of the ICT staff.

- Staff must not distribute portable storage devices that have been left in the IT suites by pupils, such as flash drives or memory sticks. If such devices are not claimed, then they will be formatted and wiped clean by the end of each school year.

- Neither pupils or staff will be allowed to install or use applications of any type from portable storage devices without express permission of the Director of ICT and the Principal.

- Pupils and staff will only be allowed to use laptops, PDAs or other computing or wireless devices to access the schools network if they can be checked prior to use by ICT staff for appropriate virus protection software or for the presence of unsuitable material. See the 'Wireless Internet Policy' for further details.

- Pupils and staff will not be allowed to use such devices to access the Internet wirelessly or by using mobile broadband within school premises or by connecting to the schools wireless network unless expressly permitted by the Director of ICT or Principal.

- In order to connect non-ENNI or non-School ICT equipment to the schools' wireless network, staff and pupils must seek permission of the Director of ICT and must sign the Wireless Internet Policy prior to use. The school is not liable for any loss or damage to pupils' or staffs' files whether caused unintentionally or by any issues caused by the incompatibility of any additional software. It is recommended that before any device is brought in to school that the staff member or pupil back-ups of all their files.

9. The Management of Risk

In common with other media such as magazines, books and video, some material available via the Internet may be unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Where there has been a deliberate attempt by a pupil to circumvent the schools' filters, e.g. through the use of a 'Proxy Avoidance' site or through the use of their own devices, access to the Internet will be withdrawn immediately and the incident will be dealt with as per the details contained herein.

9.1 Informing Students about the E-Safety and Acceptable use Policy.

- Rules for acceptable use will be posted in all rooms where computers are used.
- Students will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- Pupils will be taught the rules of positive e-communication and 'Netiquette' in year 8 as part of the ICT Key Stage 3 curriculum.

9.2 The Management of Content Filtering

- The school will work in partnership with parents, ENNI and DENI to ensure systems to protect students are reviewed and improved.
- If staff or students discover unsuitable sites, the URL (web address) and content must be reported to the Director of ICT immediately who will inform ENNI.
- The school will unblock filtered sites when it deems them useful for educational purposes having assessed the risks of allowing such access in consultation with ENNI.

9.3 Maintaining the ICT System Security.

- The school ICT systems will be reviewed regularly with regard to security and suitability for educational purposes.
- On non-ENNI PCs owned by the school, the school will ensure virus protection is installed and updated regularly. The school will purchase suitable anti-virus for PCs owned by the school and that are using the Legacy Port of the ENNI Internet connection or school Wi-Fi. ENNI provide virus protection for C2K machines.

- Where pupils access the schools' network with their own equipment, and only with the required permission, it is essential that the pupil keeps the virus protection up to date and that they comply with the terms of the Wireless Internet Policy.

- If a member of the teaching staff or technical support staff leaves the school then all administrator level usernames and passwords will be changed as appropriate including access to SIMs.

9.4 The Management of Complaints Regarding the Internet.

- Responsibility for handling incidents will be delegated to the Director of ICT. The Director of ICT will liaise with the classroom teacher, members of the Safeguarding Team, and the Year Head where necessary.

- Any complaint about staff misuse must be referred directly to the Principal.

- Any issues of misconduct that relate to Child Protection will be referred to the Safeguarding Team. See the e-Safety Policy.

9.5 Enlisting Parental Support.

- Parents' attention will be drawn to the School Internet Policy at parents evenings and through the permission letter sent out to the parents of year 8 pupils.

10. Social Networking Sites

10.1 Educational use of Social Networking Sites

- The school recognises there are many positive educational benefits of social networking sites. Whilst all such sites are currently automatically banned in school by the ENNI filtering policy, the school recognises that many pupils use such sites on a regular basis from home for educational and non-educational purposes.

- The school also recognises that pupils must be made aware of the skills needed to use such sites effectively and appropriately to enable them to participate in a global society. These skills will be highlighted through the curriculum and Pastoral programme.

- The school will aim to educate parents, teachers and pupils of the positive use of social networking sites by offering support through the schools website, school newsletters, school communications, PSNI visits, and / or via the pastoral program or through the delivery of the curriculum. In particular the school will:

    - Provide pupils with practical strategies to help them avoid giving away private information.

    - Encourage the use of social networking sites in school in order to train students in their proper use (through the schools GOOGLE CLASSROOM and targeted assemblies).

    - Ensure that students fully understand that it is not easy to delete all traces of oneself from an online community, because of comments left on other people's blogs or profiles or the interconnected nature of social networking sites.

    - Encourage teachers to join online communities for the purpose of CPD. Taking part in an online community would help teachers to understand their students' experience.

- Social Networking is an ideal medium for 'co-constructive' learning, for sharing ideas, working collaboratively, reflecting on work, and for constructively criticising work. To this effect facilities exists within our GOOGLE CLASSROOM that mirror social networking sites, in a safe educational environment.

- The school reserves the right to set up a social networking site for pupils to use in school. Such sites, available through the schools GOOGLE CLASSROOM, will be moderated by staff to ensure appropriate use.

10.2 Dealing with Incidences of Social Network Abuse

- Any attempts to access social networking sites by circumventing the schools filters, using mobile devices or mobile internet in school, or through the use of anonymous proxies, will be dealt with as "serious misconduct". Any such issues must be reported to the Director of ICT and will be fed into the existing pastoral system on a case-by-case basis.

- The school will investigate and take very seriously incidents of online bullying of pupils by pupils through social networking sites or via mobile devices when brought to our attention by staff, parents or pupils.

- If the school feels that a pupil has brought its reputation into disrepute by publishing online unsuitable comments, images, videos or voice recordings about or of pupils or members of staff, or through publishing unsuitable materials that may appear to be linked to the school, or identify the school in any unfavourable way, or posting materials online with the aim of bullying, humiliating, or intimidating any member of the school, then these matters will be investigated and suitable sanctions imposed. In extreme cases the social networking site in question and the Police will be contacted to have the material removed.

- In such cases were the pupil is found to have broken the schools code of conduct, this will be considered "serious misconduct" and will be dealt with appropriately. Sanctions may include suspension or expulsion.

- Such incidents that occur inside school, and incidents related to school occurring outside of school, should be reported to the Director of ICT, a member of the SLMT, and the Safeguarding Team. Where this involves staff or other adults working in the school this must be reported to the Principal.

- Advice for staff and young people regarding social networking sites is available here: **http://www.thinkuknow.co.uk/**

10.3 Parents role in ensuring the safe use of social networking sites at home

- Parents are encouraged to closely monitor the use of the Internet and social networking sites by their children.

- Parents are advised to place computers within a 'public' space in the house to ensure easy monitoring of online activities. Where this is not possible parents are encouraged to purchase software that will monitor their child's Internet and social networking activity such as "Net Nanny". (**http://www.netnanny.co.uk/**)

- If parents have issues concerning child protection or the posting or viewing of unsuitable content by their child or by other children or adults about their child, then they should firstly report this activity via the website in question, or where available through the

CEOP link commonly found on most websites. (**http://www.ceop.police.uk**). Parents are also encouraged to inflammatory or hurtful comments to the Police.

- Where issues of cyber bullying occur or where the school has been brought in to disrepute through such sites, the school should be informed immediately where this involves our own pupils.

10.4 Staff use of Social Networks – Summary Policy

Rationale: This policy is designed to offer guidance and to protect **staff** when using Social Networking platforms. Staff should also refer to the schools' full ICT acceptable use policy.
It is recognised that many adults working in schools use the web and social networking services such as Facebook for personal use. Whilst school employees are private individuals, and have the right to use such services to communicate and share with friends and relatives across the globe, they also have professional reputations and careers to maintain.

10.4.1 Staff must not add current students to their online social networks except when using school social networking facilities via the GOOGLE CLASSROOM.

10.4.2 Staff must not add past pupils to their online social networks as this may inadvertently provide indirect links to current students through siblings.

10.4.3 Staff must take steps to ensure that their personal data is not accessible to anybody who does not have permission to access it.

10.4.4 Staff are advised to block the sharing of their information with "friends of friends". Once information is posted on the Internet it enters the public domain. This information can be easily shared with others without your consent or knowledge.

10.4.5 All staff need to be aware that their social networking profile is public and that other users may use searches to find on-line information about staff. All staff must ensure that publicly available information about them is accurate and appropriate for viewing by a whole school audience. Inappropriate content or material that is unprofessional or that contains content which is defamatory towards the school or any of its stakeholders is a disciplinary matter that will be dealt with by the Principal and Board of Governors.

10.4.6 Staff are advised to ensure that they enable all privacy and security settings on their social networking accounts, including the prevention of messages being sent to them as a result of an unsolicited internet search. This will prevent young people accessing and potentially misusing their personal information, or making inappropriate contact.

10.4.7 All adults working in St Louis grammar School are advised to deny access as 'friends' to parents of students. It is recognised that there will be rare occasions where students or parents are close personal friends or relatives of adults working in St Louis Grammar School and staff are advised that to consider carefully these situations.

10.4.8 It is advisable that staff create and use a specific school account for interacting with the schools Twitter or other social media internet pages so as to keep separate their school and private comments.

10.4.9 All school related electronic communications should be made using official school methods. If it is necessary in an emergency to use a personal mobile or landline, then colleagues are encouraged to use141 before dialing to protect their mobile or landline number.

10.5 – Advice To Staff Who Are Subject To Having Unpleasant Comments Posted On Public Websites

If staff are aware that unpleasant comments have been posted on the internet about themselves then in the first instance staff must report such abuse to the Principal. Below is a guide as to how to 'report abuse' for the most popular websites. This has been derived from NAHT advice.

Facebook

There is now a 'report abuse' button on its pages. However, many staff will not be account holders. In this circumstance you are advised to follow this link:**http://www.facebook.com/help/contact.php?show_form=report_tos_violation**

You can find Facebook's 'Statement of Rights and Responsibilities' here:
http://en-gb.facebook.com/terms.php?ref=pf

Twitter / X

The terms of service are not as clear as others regarding abusive comments. There is reference to 'specific threats of violence' and 'You may not use our service for any unlawful purposes'. However, there are tight definitions of what constitutes violent threats. To further complicate matters one needs to be a Twitter member to make a complaint.

You Tube

To report an inappropriate video on YouTube, you need to create a free account, log in, then click the 'Flag' link under the video. To report any abuse issues on the site, go to YouTube's Abuse and Policy Centre where you can choose from a number of options related to inappropriate content, abusive users, video takedowns and privacy issues:

http://help.youtube.com/support/youtube/bin/request.py?hl=en&contact_type=abuse&rd=1

You can find YouTube's Community Guidelines here:

http://www.youtube.com/t/community_guidelines

See the Social Media Policy for more details

11. Management of the School Website Content

- The point of contact on the school website should be the school address, school e-mail (**info@stlouis.org.uk**) and telephone number. Staff or pupils' home information will not be published.
- All news stories or articles published on the school website will be first evaluated by the Publicity Officer and a member of the SLMT. (See the Publicity Policy for more details).
- Heads of department are responsible for ensuring their subject specific web pages are kept up to date. These will be reviewed on an annual basis and the Director of ICT will update the pages on request.
- Website photographs or video that includes pupils will be selected carefully. Pupils' full names will not be used anywhere on the Website in association with photographs or video.
- Parents may contact the school through the online contact form on the website though the preferred means of contact will be by telephone or, in the case of pupil absence, through Group Call (text message).
- Parents are asked for written permission at the start of year 8 before photographs or video of pupils are published on the school Website. The school and Publicity officer will ensure that photographs / videos of pupils who are not given permission to be included in school publicity are not used.

12 Printing credits

- The school operates a 'Printing Credits' system in which all pupils are allotted an adequate number of printing credits for the school year, renewed on an annual basis. This system has been put in place to help dissuade pupils from needlessly printing work or from printing materials of a non-educational nature. More detail can be found in the Ink and Paper Policy.

13. Staff use of iPads

St Louis Grammar School introduced iPads for staff in Term 1 of 2013.

Rationale:

The use of a school provided mobile device/ iPad will enhance everyday teaching and learning and will help:

- raise educational attainment
- raise levels of engagement, motivation and interaction.
- improve self-management
- create a pupil-centred curriculum based on electronic resources and e-learning
- promote remote learning / online marking / etc.
- improve facilitation of visual, audio and kinaesthetic learning styles
- meet parental / pupil demand for a move towards electronic teaching and learning
- allow access to the most up-to-date educational resources anytime / anywhere
- teaching and learning to operate within a medium that our pupils are growing up with
- provide engaging, pupil centred lessons
- allow teachers to work smarter, not harder
- improve staff IT skills

13.1 Precautions

Staff will be provided with a school iPad for educational use only. Each iPad will be individually numbered and assigned to one staff member only. The care and upkeep of the iPad will be the staff members' sole responsibility. iPads that are broken, or fail to work properly may be covered under the extended warranty / insurance policy, subject to terms and conditions.

The following general precautions must be followed:

- iPads must never be left unattended or in any unsupervised area.
- iPads must be left in a secure location at break-time and lunch time
- A protective case must be purchased and used with the iPad at all times. The case must have sufficient padding to protect the iPad from normal treatment and provide a suitable means for carrying the device within the school.
- The screens are particularly sensitive to damage from excessive pressure on the screen. Staff must avoid placing too much pressure and/or weight (such as folders and workbooks) on the iPad screen. The iPad screens can be damaged if subjected to rough treatment.
- iPads must be password protected. Staff are prohibited from sharing their password with anyone else, including pupils.
- Staff should not allow pupils unsupervised access to their iPad.

- Staff are responsible for reporting a lost, stolen or damaged iPad immediately.

13.2 The monitoring of iPads by the ICT department

All iPads should have "Find my iPad" turned on so that if lost this will allow the ICT staff to recover the iPads. Further, the IT department will annually:

- Install software on an iPad
- Monitor what software is installed on the iPads
- Secure iPads including wiping iPads if they are stolen
- Monitoring iPad usage

Staff are not permitted to remove any software the IT department may use to monitor the use of staff iPads at any time.

13.3 Use of iPads on the St Louis Wi-Fi Network and use at home

13.3.1 Staff will be able to use their iPads on the St Louis Wi-Fi network. This may enable access to websites that are not available through the normal wired network. Staff must ensure that students do not get unsupervised access to the iPads to prevent access to unacceptable content.

13.3.2 All staff must set up an Apple ID, this is a free, and staff must use their school email to set up this account. Staff may install personal content and software from the Apple Store (apps, music, other paid for content) using their own Apple account as long as it is appropriate for the school environment.

13.3.3 Any content installed by a teacher that is deemed inappropriate or illegal will be removed by the St Louis IT staff and costs incurred by a teacher for the content will not be recoverable. For example: a teacher downloads an iPad app and pays £1.99 for the app. The ICT department determines the app contains inappropriate content (sexually explicit, obscene, etc.) and removes it. The teacher will not be reimbursed for the app he/she purchased.

13.3.4 The school will install software using the schools' Apple account across all iPads. If a member of staff finds a suitable piece of software that they believe will enhance teaching and learning, a request can be made to install this software on a departmental iPads or across the whole school. Contact the Business Manager to arrange purchase of such software. This will be installed by the ICT department only. If the software is only appropriate for a single department then this may have to be purchased out of departmental funds.

13.3.5 Any content stored on the iPad must be appropriate and legal so therefore use of camera and video apps on the iPad must be in accordance with child protection policies. Photographs and videos taken during the school day must be educational in nature and purpose.

13.3.6 The teacher assigned iPad remains the property of St Louis Grammar School.

See Appendix 4 for the 'Teacher iPad Agreement'.

13.4 School iPads for pupil use

- The school has access to a set of 30 iPads which were secured through lottery funding for adult iPad classes. These will be used in accordance with the rules outline above including the following additional information.

- The school iPads may be booked out by staff for student use using the schools online booking system. **http://www.stlouis.org.uk/booking**

- Staff must monitor pupil use carefully. In particular staff must ensure:

    - They monitor pupils use of the in-built recording devices on the iPad such as the camera or audio recording facilities. These must only be used with express permission by the teacher and in accordance with this policy and the schools positive discipline policy.

    - Pupils do not install or delete Apps from the iPad from the Apple app store. This includes free games that pupils may install on their own account.

    - Pupils do not add a PIN locks to the iPad (Which means no others can get in to the iPad without knowing the number) or set alarms.

    - Pupils do not put in their own iTunes account details to download said games.

    - Pupils must not take pictures with the camera and making these pictures the wallpaper.

If a staff member want pupils to save work done on the iPads they must get pupils to email themselves by using the school email or other suitable means. However, the iPads are not set up for personal use so this is to be discouraged, particularly as other pupils may have access to the work on the iPad during the day.

13.4.1 Management of the schools' iPads

- The ICT technician will monitor and manage the schools' iPads as outlined above for staff iPads

- The school will purchase "Volume licences" to allow the easy management of the iPads. This will also facilitate the installation of software over-the-air.

- The iPads will be wiped on a regular basis.

Appendix 1 – Communication to parents

May 2016

Dear Parents

Responsible Internet Use

As part of the school's ICT Programme we offer pupils access to the Internet, the global network of computers. Before being allowed to use the Internet, all pupils must obtain parental permission. Both you and your child must sign and return the enclosed forms as evidence of your approval and their acceptance of the school rules on this matter.

We believe that effective use of the World Wide Web, e-mail and monitored discussion forums is worthwhile and is an essential skill for children as they grow up in the modern world. Such access will enable pupils to explore thousands of libraries of knowlegde, while exchanging messages with other experts throughout the world. These skills prepare them for the workplace. The school also provides a Virtual Learning Environment (GOOGLE CLASSROOM) that provides lesson and support materials for pupils that can be accessed in school and from home. This resource is maintained by teachers.

Please read the attached **Responsible Internet Use Policy** and **GOOGLE CLASSROOM Code of conduct.** Please sign and return the consent forms so that your child may use the Internet and GOOGLE CLASSROOM in school. If you wish to see a full copy of the school's **'E-Safety and Acceptable Use Policy'** and **'GOOGLE CLASSROOM Policy'**, they are available on the school website or can be provided by post. Visit the schools website for more detail.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce the risk in school. Our Internet Service Provider (ENNI) operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we have provided references to information on safe Internet access on the school website in the ICT subject area (**http://www.stlouis.org.uk/e-safety.php).**

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature and content of materials accessed through the Internet.

Our aim for Internet, discussion forum and e-mail use is to further educational goals and objectives and we believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages.

Further information has been included with this letter for parents in the form of an advice leaflet which outlines dangers that may be associated with chat rooms, instant messengers (e.g. MSN) or social networking sites such Facebook which allow children to upload their own images or create their own website. It would be advisable to discuss this with your child.

If you have any concerns about your son's / daughter's Internet use at home then please feel free to contact us at any time. It is important to note that, as not all pupils have access to the Internet at home, it is unlikely that Internet-based homework will be set by teachers. If such homework is set it can be completed within school either before school, during breaks and lunchtimes and after school.

We would be grateful if you and your son / daughter would sign the Responsible Internet Use Policy and return it to the school along with the other documentation.

If you have any comments or suggestions you would like to make regarding the Responsible Internet Use Policy please forward them in writing to me by the 23rd September 2016.

Yours sincerely,

Mr K Martin
Principal

Further contact details:
School e-mail address
info@stlouisgrammar.kilkeel.ni.sch.uk

Director of ICT and e-learning:
Mr T Brown - e-mail: **tbrown353@stlouisgrammar.kilkeel.ni.sch.uk**

Head of Junior School – Mrs B Cunningham

Year Head – XXX

Safeguarding Team – Miss C King
Mr K Martin
Mr E McGlue
Mr T Brown
Mrs B Cunningham

Advice for Parents

Your child must be careful when chatting online or when putting their personal details on the Internet. The following advice may help.

- ☑ Children should be careful who they trust online and remember that online friends are really strangers. People online, no matter how long they have been talking to them or how friendly they are, may not be who they say they are.
- ☑ Meeting someone they have only been in touch with online is dangerous. For their own safety they must always tell their parent or carer if they are thinking of meeting someone who they have met online.
- ☑ Children must not include too many personal details on the web, such as their full name, their photograph or where they live. They should use a nickname, not their real name, and a nickname that is not going to attract the wrong type of attention.
- ☑ If they use online chat, they must stay in charge! They must keep their personal information secret when chatting online (name, address, telephone number, mobile number, private email address, picture), even if people ask for this. Although it can be tempting to reveal more than they normally would in online friendships, giving out personal information can make them vulnerable.
- ☑ They must check their online profile and make sure it doesn't include any personal information (name, address, telephone number, mobile number, private email address, picture). Remember anyone can get access to their details! They must also take steps to review their safety settings. Help and advice is often included on social networking sites such as Facebook.
- ☑ If chatting online or if they have their own webpage they must keep away from unpleasant subjects or situations. If they have any worries then they should inform their parents, carer or a teacher.
- ☑ They should look out for friends and do something if they think that they are at risk.
- ☑ They should tell their parents if someone or something makes them feel uncomfortable or worried.
- ☑ They should check they know how to report something they feel uncomfortable about to the chat room / website provider or moderator.

Appendix 2 – Rules for Staff and Pupils

The computer system is owned by the school. This Responsible Internet Use statement helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

1. The school computer and Internet access must only be used for educational purposes by staff and pupils.
2. Network access must be made via the user's authorised account and password, which must not be given to any other person. Passwords must not be easy to guess. You must not attempt to access any other users work area.
3. Staff and Pupils are responsible for all material in their allocated work area and must not download or store unsuitable materials [1]. Any such material found in a work area will be saved as evidence and the person who is responsible for that work area will be locked out of the system until the matter is investigated.
4. Copyright and intellectual property rights must be respected.
5. Only school e-mail accounts should be accessed by pupils. All e-mails should be written carefully and politely respecting 'Netiquette', particularly as messages may be forwarded or printed or be seen by unexpected readers. Users are responsible for e-mails they send and for contacts made. Staff and pupils should not open attachments from unknown senders or that they suspect may contain viruses. Anonymous messages and chain letters are not permitted.
6. The use of unauthorised chat rooms is not allowed.
7. The school ICT systems may not be used for private purposes, unless the Principal has given permission for that use.
8. Use for personal financial gain, gambling, political purposes or advertising is not permitted.
9. Staff or Pupils are not permitted to install applications or '.exe' files without permission of the Director of ICT.
10. ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.
11. Any person contravening the above will forfeit their access to the Internet and the school network and may be subject to further disciplinary measures.

[1]Unsuitbale material includes materials of a Pornographic, racist, sexist or material likely to offend or corrupt; Games and "Exe" files including screen savers; Any material not associated with school work / coursework. The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix 3- Consent form

Please complete, sign and return to your ICT teacher by Friday16th September.

Pupil:	**Tutor Group:**
Pupils Agreement I have read and I understand the school rules for 'Responsible Internet Use'. I will use the computer systems and Internet in a responsible way and obey these rules at all times.	
Signed:	**Date:**
Parent's Consent for Internet Access I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from the use of the Internet facilities.	
Signed:	**Date:**
Please Print Name:	
Parents Consent for Web Publication of Work, Photographs and video. I agree that, if selected, my son / daughter's work may be published on the school web site. I also agree that photographs or video that includes my son / daughter may be published subject to school rules that photographs / video will not clearly identify individuals and that full names will not be used	
Signed:	**Date:**

Appendix 4 – teacher iPad Agreement

iPad ID: _____

Staff must agree to and sign this agreement before getting a school iPad:

1. iPads must never be left unattended or in any unsupervised area.

2. iPads must be left in a secure location at break-time and lunch time.

3. A protective case must be purchased and used with the iPad at all times. The case must have sufficient padding to protect the iPad from normal treatment and provide a suitable means for carrying the device within the school.

4. Staff must avoid placing too much pressure and/or weight (such as folders and workbooks) on the iPad screen. The iPad screens can be damaged if subjected to rough treatment.

5. iPads must be password protected. The 8 character password generated by the ICT department must be used and not changed. Staff are prohibited from sharing their password with anyone else including pupils.

6. Staff should not allow pupils unsupervised access to their iPad.

7. Staff are responsible for reporting a lost or stolen iPad immediately.

8. Staff must agree to the electronic monitoring of iPads. This is enabled through the Meraki software from Cisco. Therefore this software may not be removed.

9. Staff must agree to hand over the iPad for routine maintenance twice throughout the year (September / June).

10. Staff must agree to set up an Apple ID using their school email address for the purchase of their own apps / music / content. All material purchased must be appropriate for the school environment.

11. Any content installed by a teacher that is deemed inappropriate or illegal will be removed by the St Louis IT staff and costs incurred by a teacher for the content will not be recoverable. For example: a teacher downloads an iPad app and pays £1.99 for the app. The ICT department determines the app contains inappropriate content (sexually explicit, obscene, etc.) and removes it. The teacher will not be reimbursed for the app he/she purchased.

12. The school will periodically install software using the schools' Apple account across all iPads.

13. The teacher assigned iPad remains the property of St Louis Grammar School.

Signed: _____ **Date:** _____