St Katherine's School

ICT Acceptable Use Policy

Policy Number SKP C 005

Next Review: July 2022

Signed :	**Justin Humphreys** **Headteacher**	**Dated :**	**18.11.21**
Signed:	**William Harding** **Chair of Governors**	**Dated :**	**18.11.21**

1 Introduction

1.1 The purpose of this document is to ensure that all users (staff, students and temporary staff) of St Katherine's School computing facilities are aware of St Katherine's School policies relating to their use. Effective and proper use of information technology is fundamental to the successful and efficient running of St Katherine's School. However, misuse of information technology - in particular misuse of e-mail and access to the Internet - exposes both St Katherine's School and all users to liability and is a drain on time and money. It is critical that all users read and understand this document and make themselves aware of the risks and exposure involved.

1.2 It is the responsibility of all users of St Katherine's School computing facilities to be aware of and follow all St Katherine's School ICT policies and guidelines and to seek advice in case of doubt.

1.3 This policy may be updated or supplemented by specific standards or procedures to reflect further developments in technology or legislation or other relevant changes.

1.4 St Katherine's School encourages the use of the computing facilities for the mutual benefit of St Katherine's School and its staff. Similarly, the regulations that constitute this policy seek to provide for the mutual protection of St Katherine's School and the rights of its staff.

1.5 Consequences arising from the breach of school and ICT AUP rules and guidelines, by Students, shall be supported by the Behaviour Management system.

1.6 Consequences arising from the breach of school and ICT AUP rules and guidelines, by Staff, shall be supported by the SLT led disciplinary procedure.

1.7 Reference can be made to the SWGfL website which has resources and policy templates for ICT Acceptable Use and eSafety.

2 Computing Facilities

Access to computing facilities is managed by ICT Support. Use of any of St Katherine's School's computing facilities is at the discretion of St Katherine's School.

2.1 Definition

The phrase 'Computing Facilities' as used in this policy shall be interpreted as including any computer hardware or software owned or operated by St Katherine's School and any allocation of time, memory, disk space or other measure of space on any of St Katherine's School's hardware, software or networks.

2.2 Ownership

Computing facilities owned by St Katherine's School and software and/or data developed or created (for whatever reason) on that equipment remains in all respects the property of St Katherine's School. The Patents Act 1977 and the Copyright, Designs and Patents Act 1988 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the school.

2.3 Desktop PCs

Desktop PCs are a critical asset to St Katherine's School and must be managed carefully to maintain security, data integrity and efficiency. Therefore users must not attempt to install non-standard software on computers managed by ICT Support. Non-standard software shall be interpreted as any software that does not comply with the regulation of sub-section 2.5 below. For clarification of a machine's status as a 'Desktop PC' please consult ICT Support.

Desktop PCs include the CPU/hard-drive unit, monitor and peripherals all of which are asset components and are subject to change control. Users must contact ICT Support in order to perform a 'swap' of these assets. Any damage to these components should be reported immediately and any necessary behaviour management steps taken.

2.4 Portable Devices

Portable PCs are at high risk from loss or theft and require additional security protection. All reasonable precautions must be taken to ensure that hardware is stored securely. Also, to protect the integrity of St Katherine's School systems and data procedures, passwords or authentication devices for gaining remote access to St Katherine's School systems must not be stored with the computer. They must not be shared with other students or members of staff. Where devices are used away from the school site this should be in a secure location such as home. Devices should never be used or stored in any public areas.

School Provided Equipment

If your Portable device is lost or stolen ICT Support and the Assistant Headteacher must be notified as soon as possible. Any theft occurring away from St Katherine's School site must be reported to the Police by the user responsible, who must obtain a Police Crime Reference Number.

Personal Equipment and Devices

It is recognised that staff and students may have their own devices which they wish to use within school and for school work. Ownership and subsequent use within school however is not a right to access the network without fulfilling specific criteria, which protects the School's network and the individual's equipment.
The Bring Your Own Device (BYOD) Policy SKP A034 covers the use of personal equipment

within school and must be read and adhered to. You must only join the BYOD network with your device, unless otherwise authorised by ICT Support. Hacking or attempting to gain unauthorised access to the network will be dealt with severely through appropriate disciplinary guidelines and the behaviour policy.

Staff and guests must sign the Staff Personal Device Agreement and abide by the policy. 6th Form students and other students with permission from the SENCO must join the BYOD network only to access to the network and filtered internet connection.

Access to shared drives, data and printers is strictly forbidden under normal circumstances. This is to maintain the integrity of the files and data held on the network.

The Data Protection and Security Policy must be followed at all times and sensitive personal data should not be stored on personal devices. If using a mobile device, such as phone or tablet, with an skdrive.org Google account, ICT Support reserves the right to block or wipe your device in accordance with this policy. This is enforced through Google's Device Policy.

2.5 Software

Non-standard or unauthorised software can cause problems with the stability of school computing hardware and it is necessary to contact ICT Support before attempting to procure such software. Only software properly purchased and/or approved by ICT Support may be used on School hardware.

Whilst it is the user's responsibility to take reasonable care over the use of computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above are encouraged to contact ICT Support who will be happy to assist in resolving any issues.

Software or shareware, approved by ICT Support, may be downloaded from the Internet or loaded from other sources (e.g. CDROM) when necessary, however it is the responsibility of the individual to ensure that any licensing issues are addressed promptly, either by on-line registration or the purchasing of a valid licence through ICT Support.

In order to comply with copyright laws ICT Support must be notified when such additional or new software is installed.

The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licences must always be adhered to.

2.6 Data security

The Data Protection and Security Policy SKP C006 must be referred to in conjunction with this policy.

Users must only access information held on St Katherine's School's computer systems if they have been properly authorised to do so. Shared data areas on the server exist where departments are required to share files, carry out work or contribute to project collaborations.

If there is any doubt about access rights, to any data area, please contact ICT Support and/or the project coordinator responsible for the data to be accessed.

Under no circumstances should any user; disclose personal or other confidential information

held on computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.

It is school policy for users to store data on a network drive where it is regularly backed up.

Sensitive personal data must not be stored on a memory stick or unencrypted device.

2.7 Personal data and the Data Protection Act

St Katherine's School maintains a notification to the Information Commissioner's Office (ICO) in compliance with GDPR and the Data Protection Act 1998. This notification is held on a public register and contains details of the organisations holding and processing of personal data.

The Data Protection Officer must be informed of all collections of personal data through the annual audit. It is the responsibility of all St Katherine's School staff to ensure that personal data is held and processed within the terms of St Katherine's School's notification and in compliance with the data protection principles.

Personal data shall be:
- obtained and processed fairly and lawfully
- held for specified lawful purpose(s)
- not used or disclosed in a way incompatible with the purpose(s)
- adequate, relevant and not excessive for the purpose(s)
- accurate and up to date
- not kept longer than necessary
- available to the data subject
- kept secure.

Staff should note that all data and correspondence, including e-mail messages, held by St Katherine's School may be provided to a data subject, internal or external, in the event of a subject access request.

2.8 Camera and Recording Devices

Generally photographs for school use and those that appear in the press are a source of pleasure and pride. They enhance self-esteem for children and young people and their families and this practice should continue within safe practice guidelines. Photos and videos of staff and students are personal data and are covered under the Data Protection Act 2018.

Parental Consent

Consent is requested from parents / carers in the parent information pack sent out when a student joins St. Katherine's School. Additionally, this is updated yearly by an opt-out form sent home with the school newsletter.

Webcams and Videoconferencing

Using webcams in the classroom opens up a range of teaching and learning possibilities. The Data Protection Act 2018 applies in the same way as photography. Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a video, this will usually be enough to ensure compliance.

School Cameras

Photographs and videos can be taken with school provided equipment provided the images are

processed and stored in line with the Data Protection Act.

Personal Cameras
Personal devices should not be used to take images of pupils or staff.

2.8 Freedom of Information Act
St Katherine's School is subject to the provisions of the Freedom of Information Act (2000) which provides for the general right of access to information held by public authorities. While St Katherine's School is in the process of meeting the requirements of the Act, staff should be aware that the Act effectively extends rights available under the Data Protection Act to include all types of information held, whether personal or non-personal. Therefore, such data or correspondence may be provided to an applicant in the event of an access request once the Act has come into force. Further information about this Act may be obtained from the Stationery Office Limited as the **Freedom of Information Act 2000**, (ISBN 0 10 543600 3)

2.9 Virus protection
Anti-virus software is loaded on all computers as standard and is updated regularly via the network. Anti-virus software must not be de-installed or deactivated. Files received by or sent by e-mail are checked for viruses automatically. Remote users are responsible for maintaining up to date virus definitions on their computers and can contact ICT Support for help as required. Users must not intentionally access or transmit computer viruses or similar software. Non-St Katherine's School software or data files intended to be run on School equipment by external people such as engineers or trainers must be checked for viruses before use. If you suspect that a virus has infected a computer then stop using the computer and contact ICT Support immediately.

2.10 Network access
Passwords protect St Katherine's School systems from access by unauthorised people: they protect your work and the school's information. Therefore never give your network login id or password to anyone else. Automatic procedures are in place on systems to ensure users change passwords on a regular basis, passwords are of a minimum length and old passwords cannot be reused immediately. Passwords must be six or more characters long and include at least one numeric or non-alphabetic special character. St Katherine's School does not allow the connection of non-approved computer equipment to the network without prior written request and technical approval.

2.11 Further general guidance
St Katherine's School users must ensure prior approval from the ICT Network Manager to:
- set-up hyperlinks to world wide web sites on St Katherine's School computing facilities
- publish pages on external world wide web sites containing information relating to St Katherine's School
- enter into agreements on behalf of themselves or St Katherine's School via a network or electronic system
- transmit unsolicited commercial or advertising material to other users of a network or to other organisations
- be used for external business interests or personal gain

3 Electronic mail

3.1 Use and responsibility

St Katherine's School's electronic mail (E-Mail) system is provided for the school's business purposes. E-mail is now a critical business tool but inappropriate use can expose St Katherine's School and the user to significant liability.

Liability can arise in a number of ways including, among others, copyright or trademark infringement, misuse of confidential information, defamation and liability for inaccurate statements.

The e-mail system must be used judiciously in the same manner as other school resources such as telephones and photocopying.

3.2 Content

E-Mail messages must be treated like any other formal written communication. E-Mail messages cannot be considered to be private, secure or temporary. E-Mail can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.

Improper statements in an E-Mail can give rise to personal liability and liability for St Katherine's School and can constitute a serious disciplinary matter. E-Mail that embarrass, misrepresent or convey an unjust or unfavourable impression of St Katherine's School or its business affairs, staff, suppliers, customers or competitors are not permitted. Do not create or send E-Mail messages that are defamatory. Defamatory E-Mail whether internal or external can constitute a published libel and are actionable. Never send confidential or sensitive information via E-Mail. E-Mail messages, however confidential or damaging, may have to be disclosed in court proceedings. Do not create or send E-Mail messages that may be intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability. It is never permissible to subject another student or member of staff to public humiliation or ridicule; this is equally true via E-Mail. Copyright law applies to E-Mail. Do not use E-Mail to transmit or circulate copyrighted materials.

3.3 Privacy

E-mail messages to or from users cannot be considered to be private or confidential. Although it is not policy to routinely examine the content of individuals E-Mail, St Katherine's School reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or some legal obligation to do so. Good cause shall include the need to fulfil school obligations, detect employee wrongdoing, protect the rights or property of the school, protect IT system security or to comply with legal process.

Messages sent or received may be copied and disclosed by the school for lawful purposes without prior notice.

It is not permissible to access or to send E-Mail from another employee's personal account either directly or indirectly.

3.4 Non-School provided email
St. Katherine's School provided an email account for all staff and students. Staff must not use a non-school provided account to contact pupils or parents or to conduct school business. Further information can be found in the Social Media Policy SKP C013

3.5 Exams
A candidate is eligible for word processor when it is their normal way of working AND when it is appropriate to their need. A candidate must be confident in the use of a memory stick to save their work to be awarded a word processor. This includes candidates with:

• A learning difficulty which has a substantial and long-term adverse effect on their ability to write legibly

• A medical condition

• A physical disability

• A sensory impairment

• Planning and organisational problems when writing by hand

• Poor handwriting, deemed illegible, very disorganised, or very messy by at least two separate staff members.

A laptop cannot simply be granted to a candidate because they would prefer to type rather than write in examinations, can work faster or because they use a laptop at home. This must be their normal way of working in tests and mock exams and will be observed before an application is made.

The SENCo confirms in writing with the student and their parent that these conditions have been met and this has been recorded on the Access Arrangements register.

4 Internet usage
The laws of all nation states regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax apply equally to online activities. However, the practical legal position regarding Internet usage is often uncertain.

Documents must not be published on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability under the sovereign law of the country in which the web server hosting the published material is sited.

Material must not be accessed from the web which would be objectionable on the above grounds under the sovereign law of the countries in which the networks transporting the material are sited or which would violate the Acceptable Use Policies of those networks.

Given the impracticality of assessing the exact legal position with regard to the previous two paragraphs, St Katherine's School Acceptable Use Policy governing material that could be objectionable on the above grounds is grounded in English law, on which basis it is reasonable

to expect St Katherine's School staff to have good awareness and to be able to exercise good judgement.

If there is any doubt over a specific case escalate through the departmental Line Manager. Once information is published on the worldwide web anyone from anywhere in the world can access it. It is therefore critical that material of a proprietary or sensitive nature should not be published on unsecured public web sites.

All Internet usage from the St Katherine's School network will be monitored and logged by the South West Grid for Learning. Reporting on aggregate usage is performed on a regular basis.

When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant user account. Such an investigation may result in action via St Katherine's School's Disciplinary Procedure and possibly criminal investigation.

Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Files so protected must never be transmitted or redistributed to third parties without the express permission of the copyright owner. Any files or software found on St Katherine's computing facilities which breach copyright rules will be removed and appropriate action taken against the user who has installed the material on the network.

4.1 Newsgroups
Postings to newsgroups are in effect E-Mail published to the world at large and are subject to the same regulations governing E-Mail as above. Always include a disclaimer with a posting if it could be interpreted as an official statement or policy of St Katherine's School. For example: "The views expressed are my own and do not necessarily represent the views or policy of my employer."

4.2 Instant messaging
Instant messaging is free, fast, real-time and powerful. However instant messaging also carries inherent risks: lack of encryption (allowing the possibility of eavesdropping) logging of chat conversations without a user's knowledge and virus risks.

Due to these risks, St Katherine's School does not allow the use of instant messaging.
The Social Media Policy (SKP C013) contains further information pertaining to the use of messaging and social networks.

4.3 Proxy Server
A proxy server is a server, sits between the user and the internet, which receives requests (such as a Web page request) from a user. The proxy server will apply filters to the request and pass back to the user the result of that request.

The filters are maintained and updated regularly by ICT Support and SWGfL Filtering. The filters are intended to reduce the risks associated with the internet use in an educational environment.

Attempting to bypass the proxy server will put individuals in breach of this policy and subject to disciplinary procedures.

Staff can apply to ICT Support for a special proxy override account known as the "Staff Proxy",

which allows unfiltered access to the internet. Access to this is logged to the individual users and is password protected. A change control form must be received before the account is enabled.

Staff must not share this staff proxy access with students or allow students to access their laptop.

4.4 Mobile Phones

Please refer to the Mobile Devices Policy SKP C018 and the Bring Your Own Device Policy.
In light of recent advances in mobile telecoms it is necessary to mention that mobile phones with contractual access to the internet fall outside of the safe and controlled environment offered by the SWGfL and School's filtering facility.

Students' use of these devices must be monitored carefully and the Uniform and Equipment Policy (SKPA029) Section 12 and the Mobile Devices Policy apply.

Where educational need and planned lesson activities require access to the internet. ICT Support will provide access for staff only via the school network. Staff must supervise students at all times and maintain vigilance for inappropriate access and/or content. Guidelines and advice can be obtained from ICT Support.

St Katherine's School cannot rely solely on reassurances from mobile ISP companies about age restricted internet access.

Eg. Some ISP companies require authorisation from an adult to access age restricted sites/content.

4.5 Social Networking Sites

Social networking websites are blocked in school by the SWGFL Web-Based Social Networking List (see Appendix 3). Access to these sites by use of a proxy-bypass website is defined as misconduct under appendix 1 and they must not be accessed in school except where required as part of school business.
Use of social networking sites is controlled both in school and out of school by the Social Media Policy (SKP C013).
Incidents of bullying taking place on social networking sites will be dealt with by the school's eSafety Officer and the normal behaviour procedures.

5 Private use, legislation and disciplinary procedures

5.1 Private use

Computing facilities are provided for St Katherine's School's business purposes and responsible personal use is allowed provided there is no conflict with the interests or requirements of St Katherine's School. St Katherine's School does not accept liability for any personal loss or damage incurred through using the School computing facilities for private use.

5.2 Updates to this Policy
In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all staff will be made when updates are available.

5.3 Relevant legislation
The following are a suggested list of Acts that could apply to the use of St Katherine's School computing facilities:
• Regulation of Investigatory Powers Act 2000
• Computers' Misuse Act 1990
• Protection from Harassment Act 1997
• Sex Discrimination Act 1975
• Race Relations Act 1976
• Disability Discrimination Act 1995
• Obscene Publications Act 1959
• Telecommunications Act 1984
• Protection of Children Act 1978
• Criminal Justice Act 1988
• Data Protection Act 2018
• The Patents Act 1977
• Copyright, Designs and Patents Act 1988
• Defamation Act 1996
• Freedom of Information Act 2000
• Human Rights Act 1998

5.4 Disciplinary and related action
St Katherine's School wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently it expects and supports the integrity of its staff. In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Appendix 1 details examples of behaviours which are unacceptable within St Katherine's School and provides examples of behaviour deemed as Gross Misconduct and Misconduct.

Appendix 2 details the rules for responsible PC use.

Appendix 3 details the Internet Filtering Policy.

Appendix 1:
Examples of behaviours which require the use of the St Katherine's School disciplinary policy

GROSS MISCONDUCT Examples.

- Criminal Acts – for example in relation to child pornography.
- Visiting pornographic sites (adult top shelf materials) except where this forms an authorised part of the staff job (for example 'investigation of incidents or allegations').
- Harassment – inappropriate e-mails or printed e-mails sent to a colleague, even if sent as a joke. Harassment can take a number of forms and is defined as unwanted conduct that affects the dignity of people within the workplace.
- Obscene racist jokes or remarks which have been shared internally and externally – reflects on the image of employer and brings the organisation into disrepute.
- Downloading and installation of unlicensed products.
- Viewing sexually explicit materials, except where this forms an authorised part of the staff job (for example 'investigation of incidents or allegations').
- Chat rooms – sexual discourse, arrangements for sexual activity.
- Violation of St Katherine's School's registration with the Federation Against Software Theft – such as software media counterfeiting or illegitimate distribution of copied software.

MISCONDUCT Examples.

- Frivolous use of School computing facilities that risk bringing St Katherine's School into disrepute. The distribution of animated Christmas card programmes or 'chain e-mails' beyond the internal e-mail system would represent examples of such misconduct.
- Entering into contracts via the Internet that misrepresent St Katherine's School. Contracts are legally binding agreements and an employee must not enter into any agreements via the Internet to procure goods or services where St Katherine's School is liable for this contract, without first consulting St Katherine's School's Financial procedures (available from Finance).
- Deliberate introduction of viruses to systems.
- Deliberate and intentional use of security / proxy bypass utilities

This list is not exhaustive, but sets the framework of St Katherine's School's approach to misuse of computing systems. St Katherine's School has the right to monitor staff use of computer equipment where there is evidence to suggest misuse.
(for example Regulation of Investigatory Powers Act 2000).

The implementation of this Policy will be monitored by the Governing Body Student Committee.

Appendix 2

Acceptable use of ICT in St. Katherine's School – Student Summary

- I will only access the ICT system with my own login and password.
  This ensures that all of your work is stored in the same place.
- I will keep my login and password secret.
  This ensures that no-one can interfere with your work.
- I will only use the computers for school work.
  This ensures that you are not preventing others from using hardware or software.
- I will not bring in or download programs for any purpose.
  This prevents the network from being corrupted.
- I will not import and/or store media files from outside school.
  Media files (e.g. mp3 music files) are governed by copyright law. They also take up scarce server space.
- I will ask permission from a member of staff before using the Internet during a timetabled lesson.
  This ensures that you are using the resources which you need for your lesson.
- I will only send email to other school email accounts (Y9-13).
  This restriction is built in to the email system.
- I will not send messages which are impolite or could cause offence.
  Inappropriate messages can cause harm and may leave you open to prosecution.
- I will only use the email client which the school has given me.
  Other email clients do not have the same level of virus checking as the school system and can damage the network.
- I understand that the school may check my computer files.
  We need to do this in order to protect our system. We will only do so if we suspect that there is a problem.
- I understand that unauthorised files may be deleted without warning.
  We will delete files which are inappropriate, which may breach copyright laws or which take up unreasonable amounts of space.
- I understand that the school may monitor PCs for inappropriate use.
  We are obliged to do this and we may use a variety of means of doing this.
- I understand that inappropriate use of ICT equipment may result in disciplinary action.
  Inappropriate use is against the schools ICT Acceptable Use Policy (AUP), and may, in extreme cases, be illegal.
- Use of social networking sites in school is not allowed.
  It is inappropriate in a school environment and is against the schools ICT Acceptable Use Policy (AUP)
- Use of Instant Messaging within school is not allowed.
  It is inappropriate in a school environment and is against the schools ICT Acceptable Use Policy (AUP)
- I will not attempt to connect to or request friendship connections with members of staff on social networking sites.
  It is inappropriate and is against school child protection guidelines.
- I will not upload images of myself or others to social networking sites without ensuring that the schools badge or logo cannot be seen either in the background or off my school uniform.
  It is quite possible that the school or an individuals location can be obtained easily.
- I WILL NOT bring the school into disrepute by adding defamatory comments about students or members of staff (past or present)
- I will not use any internet enabled devices such as PDAs, MP3 players, including any handheld gaming devices and mobile phones to access or attempt to access the internet within school.
  ICT equipment and access to the internet is provided for students and staff to research and support the needs of the curriculum
- I will report (in confidence) any unpleasant material or messages sent to me, either verbally or electronically.
  We want to protect you from harm. We will take action if we can trace inappropriate material or messages. We may have to involve you, your parents or the police to assist. The E-Safety officer is available to discuss, advise and investigate E-Safety incidents. An incident log is kept of all incidents, investigations and actions taken to protect you.

At home I will discuss the Golden rules for E-Safety with my parents

- G – Agree ground rules, privacy and boundaries for Internet use at home.
- O - Online safety, anti virus and activating security settings.
- L - Location and type of internet access in the home.
- D – Dialogue, keep talking about the sites you have seen and issues you feel confused or worried about.

Appendix 3

Internet Filtering Policy

St. Katherine's School uses the Internet filtering service launched by IFL, Internet for Learning) called SafetyNet Plus. SafetyNet Plus allows the School to override the standard RM SafetyNet service and specify the particular sites and searches to permit and deny their user's access to.

This means that decision-making is moved from IFL to the school, allowing us to tailor their Internet Filtering according to our environment and Acceptable Internet Use Policy.

RM SafetyNet Plus enables schools to:

- Deny access to a URL or part of a URL, which is otherwise permitted by IFL.
- Deny access to specific file extensions e.g. .mp3 or .exe.
- Deny access to everything, except permitted URLs (walled garden approach).
- Permit access to URLs, which are currently denied by IFL (this could be a specific chat site for example).
- Support the RULES FOR RESPONSIBLE PC USE (Appendix 2)

Access to the Internet and Email services is controlled by filtering which is applied by the South West Grid for Learning. This is designed to protect all users from illegal activity (including copyright fraud) and malicious programs.

Internet Filtering

Internet filtering applies to ALL users of the internet in school. It has three levels:

Content	SWGfL Pornography Filter List SWGfL Drugs/Substance Abuse Filter List SWGfL Intolerance Filter List SWGfL Violence Filter List St. Katherine's School Filter List
Services	SWGfL Web-Based Chat Filter List SWGfL Web-Based Mail Filter List SWGfL Mobile Phones/SMS/Ring Tones Filter List SWGFL Web-Based Social Networking List
Download	SWGfL Banned .mp3 File Download Filter List

The St. Katherine's School Filter List is the only one which can be controlled by the school.

Email Filtering - Staff

All SWGfL email is checked for viruses before being stored for users. The virus checker will not allow program files to be attached to emails. There are no other restrictions for staff.

Email Filtering – Students

In addition to virus checking, students are not allowed to send email to, or receive email from,

any account which is not in a domain ending in ".sch.uk". This prevents emails to and from personal hotmail accounts for example.