St JOHN FISHER CATHOLIC

COMPREHENSIVE SCHOOL

ICT Acceptable Use POLICY

The Mission statement:

"St John Fisher School seeks to help and encourage pupils to develop individually, collectively and freely a way of life modelled on Christ, in accordance with the Faith of the Roman Catholic Church."

Date of Policy:	November 2015
Date of Ratification:	Under review awaiting ratification.
Date of Review:	Forthcoming Faith, Mission & Ethos Governor Meeting.
Owner:	B Willsher

ICT and Learning Technology Acceptable Use Policy

Student and staff guide to the use of ICT in School

1 Equipment

1.1 Vandalism
Vandalism is defined as **any action** that harms or damages any equipment or data that is part of the School's ICT facilities. Such vandalism is covered by the Computer Misuse Act 1990. This includes, but is not limited to: · Deliberate damage to computer hardware such as monitors, base units, printers, keyboards, mice or other hardware. · Change or removal of software · Unauthorised configuration changes · Create or upload computer viruses · Deliberate deletion of files. Such actions reduce the availability and reliability of computer equipment; and puts at risk other users' data. In addition, these actions lead to an increase in repairs of the ICT facilities, which impacts upon every users' ability to use the ICT facilities. The other result of vandalism is that it incurs costs, which reduce the funds available to improve the ICT facilities the School has.

1.2 Use of Removable Storage Media
St John Fisher Catholic School accepts the fact that you may wish to transfer school work done at home to school using a flash memory device or a CD/DVD disk. However St John Fisher Catholic School cannot guarantee that your work will be able to be transferred properly using these. We therefore encourage you to use the VLE or RM Portico when transferring work between home and school.

1.3 Printers and Consumables
Printers are provided across the school for use by students. Please use the printers sparingly and for educational purposes only. Take the time to check the layout and proof read your work using the 'Print Preview' facility before printing.

1.4 Data Security and Retention
All data stored on the St John Fisher Catholic School network is backed up daily and backups are stored for at least two weeks. If you should accidentally delete a file or files in your user area or shared area, please inform the ICT Technical Staff immediately so that it can be recovered. Generally, it is not possible to recover files that were deleted more than 8 weeks previously or files which were deleted on the same day as they were created.

2. Internet and E-mail

2.1 Content Filtering
St John Fisher Catholic School provides layers of internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. If you come across any inappropriate website or

2.2 Acceptable use of the Internet

All Internet access is logged and actively monitored and they are stored for up to 3 months and usage reports can and will be provided to any member of staff upon request. Use of the Internet should be in accordance with the following guidelines:

Only access suitable material – the Internet is not to be used to download, send, print, display or transmit material that would cause offence or break the law.

Do not access Internet Chat sites. Remember you could be placing yourself at risk.

Never give or enter your personal information on a website, especially your home address, your mobile number or passwords.

Do not access online gaming sites. Remember that your use of the Internet is for educational purposes only.

Do not download or install software from the Internet, as it is considered to be vandalism of the School's ICT facilities.

Do not use the Internet to order goods or services from online, ecommerce or auction sites.

Do not subscribe to any newsletter, catalogue or other form of correspondence via the Internet.

Do not print pages directly from a website. Web pages are often not properly formatted for printing and this may cause a lot of waste. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.

2.3 Email -Students only, staff have separate policy
You will be provided with an email address by the School, and the expectation is that you will use this facility for legitimate educational and research activity. You are expected to use email in a responsible manner. The sending or receiving of messages which contain any material that is of a sexist, racist, unethical, illegal or likely to cause offence should not take place. Remember when sending an email to: · **Be Polite** never send or encourage others to send abusive messages.

Use appropriate language remember that you are a representative of the School on a global public system. What you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language.

Do not reveal any personal information about yourself or anyone else, especially home addresses, personal telephone numbers, usernames or passwords. Remember that electronic mail is not guaranteed to be private.

Do not download or open file attachments unless you are certain of both their content and origin. File attachments may contain viruses that may cause loss of data or damage to the School network.

3.0 External Services

St John Fisher Catholic School provides a number of services that are accessible externally, using any computer with an Internet connection. You should use this facility only for educational activities only and in accordance with the following guidelines:

3.1 RM Portico This service is only available to students under special circumstances and to staff who have received the CPD

Training

RM Portico provides remote access to files and resources stored on the School network, via the Internet. This service is provided to students and staff to enable them to transfer files between home and school and also to enable students to remotely access electronic lesson resources.

The use of RM Portico is subject to the following guidelines. Use of the facility is closely and actively monitored and any abuse or misuse will result in the facility being withdrawn and/or other disciplinary action being taken against you.

3.2 VLE

SJF provides a web-based portal allowing users access to personalised learning resources and lesson materials. Use of this service should only be in accordance with instructions from your subject tutor and in accordance with the following guidelines:

The VLE is provided for use of St John Fisher Catholic School staff and students only. Access by any other party is strictly prohibited with the exception of Parents and adults who have legal responsibility for pupils, who will be able to access this facility via their child's account, and in so doing are subject to the guidelines in this policy. !t a later date, when the facilities are available, it may be possible to provide parents and adults who have legal responsibility for pupils with their own account that will allow them to access information relevant to their child's educational progress.

Never reveal your password to anyone or attempt to access the service using another student's login details.

The VLE remote access service is provided by an external company for St John Fisher Catholic School can make no guarantees as to service availability or quality.

3.3 Web based E-mail – Students only, staff have separate policy

Web email provides remote access to your email account from home or anywhere with an Internet connection. Use of the facility is closely and actively monitored and any abuse or misuse will result in the facility being withdrawn and/or other disciplinary action being taken against you.

4.0 Privacy and Data Protection

4.1 Passwords

-When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name or address. Generally, longer passwords are better than short passwords. If possible include numbers and symbols in your password.

-If you forget your password, inform ICT Technical Staff immediately.

-If you believe that someone else may have discovered your password, then change it immediately and inform a member of staff.

4.2 Security

-Never attempt to access files or programs to which you have not been granted access to. Attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action.

-You should report any security concerns immediately to a member of staff

-If you are identified as a security risk to the School's ICT facilities you will be denied access to the systems and be subject to disciplinary and/or criminal action.

You should consider any access to information stored on the school computer network as unauthorised unless you have been given specific permission to access that information.

If you think you have accidentally gained access to something you probably shouldn't, you should inform your teacher or a member of the ICT technical staff immediately.

5.0 Service

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the school will not be responsible for any damages or loss incurred as a result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, non- deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions.

Use of any information obtained via the school's ICT system is at your own risk. St John Fisher Catholic School specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

Student and staff guide to the use of ICT in School

This document is to ensure the safety and wellbeing of staff and students at SJF. It is in place to ensure the users of the St John Fisher network remain staff and secure at all times.

If there are any concerns over the security of the ICT equipment please report to the Network Manager immediately.

I have read and agree to the acceptable use policy and will abide by the terms and conditions set out under the sub heading below:

1 Equipment

- 1.1 Vandalism
- 1.2 Use of Removable Storage Media
- 1.3 Printers and Consumables
- 1.4 Data Security and Retention

2. Internet and E-mail

- 2.1 Content Filtering
- 2.2 Acceptable use of the Internet
- 2.3 Email -Students only, staff have separate policy

3.0 External Services

- 3.1 RM Portico
- 3.2 The VLE
- 3.3 Web based E-mail – Students only, staff have separate policy

4.0 Privacy and Data Protection

- 4.1 Passwords
- 4.2 Security
- 5.0 Service

I will not use the schools ICT systems for any unlawful access I read and agree to follow the AUP policy and report any concerns to the network manager

I am aware the school monitors and tracks ALL internet usage, this included incoming and outgoing web based mail

Print Name:			
Signed:			
Date:		**Form Group:**	

Appendix and Notes

1.0 Computer Misuse Act 1990

The Computer Misuse Act makes it an offence for anyone to have:

-Unauthorised access to computer material e.g. if you find or guess a fellow user's password and use it. -Unauthorised access to deliberately commit an unlawful act e.g. if you guess and fellow user's password and access their account without permission. -Unauthorised changes to computer material e.g. if you change the desktop set up on your computer or introduce a virus deliberately to the school's network system.

2.0 Data Protection Act 1998

The Data Protection Act ensures that information held about you is used for specific purposes only. These rules apply to everyone in the school, including teaching staff, support staff, volunteers and governors.

The Act covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in the school. The Act not only applies to paper files it also applies to electronic files.

The Principles of the Act state that data must be:

-Fairly and lawfully processed -Processed for limited purposes -Adequate, relevant and not excessive -Accurate and up to date -Kept no longer than necessary -Processed in accordance with data subject's rights -Secure -Not transferred to other countries without adequate provision.

3.0 RIPA – Regulation of Investigatory Powers Act 2002

If a request for authorised access is made to the school they will provide the appropriate access to your ICT records and files.

The Act legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism. RIPA makes provision for:

-the interception of communications -the acquisition and disclosure of data relating to communications -the carrying out of surveillance -the use of covert human intelligence sources -access to electronic data protected by encryption or passwords

If a request for authorised access is made to the school, we will provide the appropriate access to your ICT records and files.