Saint Martin's Catholic Academy

E-Safety Policy - Acceptable Use - Students
January 2015

Why have an Acceptable Use Policy?

An Acceptable Use Policy is about ensuring that you, as a student at Saint Martin's can use the internet, email and other technologies available at the school in a safe and secure way. The policy also extends to out of school facilities e.g. equipment; printers and consumables; Internet and email; managed learning environments and websites.

An Acceptable Use Policy also seeks to ensure that you are not knowingly subject to **identity theft** and therefore fraud. Also that you **avoid cyber-bullying** and just as importantly, you **do not become a victim of abuse**. We have also banned certain proxy sites as well as anonymous proxy sites, because they put the school network at risk.

Help us, to help you, keep safe.

Saint Martin's recognises the importance of ICT in education and the needs of students to access the computing facilities available within the School. The School aims to make the ICT facilities it has available for students to use for their studies both in and out of lesson times. To allow for this Saint Martin's requires all students to sign a copy of the Acceptable Usage Policy **before** they receive their username and password.

Listed below are the terms of this agreement. All students at Saint Martin's are expected to use the ICT facilities in accordance with these terms. Violation of terms outlined in this document may lead to loss of access and/or disciplinary action, which will be taken in accordance with the Behaviour Management Policy of the School.

Please read this document carefully then sign and date the acknowledgement slip and return it to indicate your acceptance of the Policy before the start of the Autumn Term. Access to the School's ICT facilities will only take place once this document has been signed by **BOTH** the **student** and **parent/carer**.

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 (see Glossary). 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 put at risk other users' data. In addition, these actions lead to an increase in repairs of the ICT facilities, which impacts upon every student's 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

Saint Martin's accepts the fact that you may wish to transfer school work done at home to school using a flash memory device or a disk. However, Saint Martin's cannot guarantee that your work will be able to be transferred properly using these. We therefore encourage you to use the Hinckley Area Schools Partnership Virtual Learning Environment (HASP VLE) when transferring work between home and school.

1.3 Printers and Consumables

Printers are provided across Saint Martin's 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.

All printer use is recorded and monitored and therefore if you deliberately use the printer for non-education or offensive material you will be subject to the behaviour management measures of the School which includes the following:

- A warning
- Email and/or Internet facilities removed
- Letter home to parents/carers
- Loss of access to the print facilities available within the School
- Report to the School Governors
- Report to appropriate external agencies like the Police

1.4 Data Security and Retention

All data stored on the Saint Martin's network is backed up daily and backups are stored for up to at least two weeks. If you should accidentally delete a files or files in your folder or shared area, please inform the IT Technician immediately so that it can be recovered. Generally, it is not possible to recover files that were deleted more than three months previously.

2. Internet & Email

2.1 Vandalism

Filtering

Saint Martin's provides two layers of internet filtering (EMBC and Securus), 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 content whilst using the ICT equipment, you must report it to a member of staff immediately.

The use of Internet and email is a privilege and inappropriate use will result in that privilege being withdrawn.

2.2 Acceptable use of the Internet

All Internet access is logged and actively monitored (by an instant monitoring system which highlights improper use as it is happening) and records are stored for up to three weeks and usage reports can and will be provided to any member of staff upon request.

- Only access suitable material – the Internet is not 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 on-line, e-commerce 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.

Use of the Internet should be in accordance with the following guidelines:

2.3 Email

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.

- **Consider the file size of an attachment** - files exceeding 1MByte in size are generally considered to be excessively large and you should consider using other methods to transfer such files.

- **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.

2.3 External Services

Saint Martin's 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 Hinckley Area Schools Partnership Virtual Learning Environment (HASP VLE)

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

The use of HASP VLE 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.

- HASP VLE is provided for use of Hinckley Area schools (including Saint Martin's) staff and students only. Access by any other person is not allowed.
- Never reveal your password to anyone.
- HASP VLE should only be used to transfer files linked to educational, research activities or relevant to the subjects you are studying. Any other use is not allowed.
- All files must be virus checked before being transferred via EasyLink

3.2 Web-Email

EMBC email provides remote access to your email account from home or anywhere with an Internet connection. Use of this service 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.

- Web-email is provided for use of Saint Martin's staff and students only. Access by any other person is not allowed.
- Never reveal your password to anyone.
- Remember to treat file attachments with caution. File attachments may contain viruses that may cause loss of data or damage to the computer from which you are working. Do not download or open file attachments unless you are certain of both their content and origin. Saint Martin's accepts no responsibility for damage caused to any external equipment or software, as a result, of using the web-email service.

3.3 Managed Learning Environment Software

It's Learning (the company used for HASP VLE) 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:

- It's Learning is provided for use by HASP/Saint Martin's staff and students only. Access by any other party is strictly prohibited.

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

- It's Learning provide the remote access service used by HASP. Saint Martin's can make no guarantees as to service availability or quality.

4.0 Privacy and Data Protection

4.1 Passwords

- Never share your password with anyone else or ask others for their password.

- 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 you forget your password, inform the ICT Technician 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. 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 action.

4.3 Storage and Safe Transfer of Personal Data

- Saint Martin's holds information on all students and in doing so, we must follow the requirements or the Data Protection Act 1998 (see Glossary). This means that data held about students can only be used for specific purposes and therefore all data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

- Saint Martin's will seek to ensure that personal data sent over the internet will be encrypted or otherwise secured.

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 Saint Martin's ICT system is at your own risk. Saint Martin's specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

6.0 Mobile Technologies

For reasons of safety and security students should not use their mobile phone or any other technology in a manner that is likely to bring the school into disrepute or risk the welfare of a child or young person.

In order to reduce the opportunity for those behaviours that could possibly cause upset, student use of mobile phones in or around Saint Martin's school buildings and its environment is prohibited during the school day. Phone calls may be made from the School Office if necessary.

The development of mobile technology is such that mobile phones and other similar devices connected to mobile networks have enhanced features which include: picture messaging; mobile access to the Internet; entertainment in the form of video streaming and downloadable video clips from films, sporting events, music and games etc. The capabilities of 3G mobile phones also means that adults working within the school environment may be sent inappropriate images or videos, or be encouraged to send back images or video of themselves using integrated cameras.

If you are sent inappropriate material e.g. images, videos etc report it immediately to a member of staff and/or parent/carer.

Glossary

Computer Misuse Act

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

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.

RIPA – Regulation of Investigatory Powers Act

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.

REQUIRED SIGNATURES

Once you have read and understood this document, please sign and return the paper acknowledgement which you will have been given, after which time access to the school's ICT facilities will be granted.

This document will be valid for the duration of your stay at Saint Martin's.

Saint Martin's Catholic Academy

School E-Safety Policy Acceptable Use Statement – Students

STUDENT

I understand and agree to the provisions and conditions of this agreement (the full contents of which I have read on the school's website) I understand that any disobedience to the above provisions may result in disciplinary action and the removal of my privileges to access ICT facilities. I also agree to report any misuse of the system to a staff member and I understand that misuse may come in many forms but may be viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal activities, racism, sexism inappropriate language, any act likely to cause offence.

NAME (print): ……

SIGNATURE: ……

DATE: ……

FORM: ……

PARENTS/CARERS

As the parent or carer of (print)…… I have read this agreement (the full contents of which I have read on the school's website) and understand that access to electronic information services is designed for educational purposes. I understand that, whilst the Internet service provider operates a filtered service, it is impossible for Saint Martin's to restrict access to all controversial materials and will not hold the school responsible for materials acquired on the network. I also agree to report any misuse of the system to the school.

I hereby give my permission for Saint Martin's to permit my child access to electronic information services and I certify that the information given on this form is correct.

NAME (print): ……

SIGNATURE: ……

DATE: ……