Authorised Acceptable Use Policy (Staff, Governors and Volunteers)

Why have an Authorised Acceptable Use Policy?

An Authorised Acceptable Use Policy is about ensuring that you, as a member of staff/volunteer/Academy Governor at Saint Martin's Catholic Academy can use the Internet, email and other technologies available at the Academy in a safe and secure way. The policy also extends to out of Academy facilities e.g. equipment; printers and consumables; Internet and email, managed learning environment and websites.

An Authorised 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 sites which put the Academy network at risk.
Help us, to help you, keep safe.

Saint Martin's Catholic Academy strongly believes in the educational value of ICT and recognises its potential to enable staff and volunteers in delivering and supporting the curriculum. Saint Martin's Catholic Academy also believes that it has a responsibility to educate its pupils; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and other related technologies. To this end the expectation of Saint Martin's Catholic Academy is that both staff and volunteers will play an active role in implementing Academy and departmental Internet safety polices through effective classroom practice.

Saint Martin's Catholic Academy recognises that for staff and volunteers to effectively deliver and support the curriculum they must be able to make use of the ICT facilities of the Academy and have the opportunity to expand and develop the teaching material associated with their work. However, Saint Martin's Catholic Academy expects that both staff and volunteers, will at all times, maintain an appropriate level of professional conduct in their own use of the Academy's ICT facilities.

Listed below are the terms of this agreement. Staff, Academy Governors and volunteers are expected to use the ICT facilities of the Academy in accordance with these terms. Violation of these terms is likely to result in disciplinary action in accordance with the Academies Disciplinary Procedures. Where the policy is breached in by either volunteers or governors the Academy will seek to advice and support from St Thomas Aquinas Multi-Academy Catholic Trust in order to manage the situation in a fashion that safeguards the Academy population.

Please read this document carefully and sign and date it to indicate your acceptance of the terms herein.

1. Equipment

1.1 Academy Computers

All computers and associated equipment are the property of Saint Martin's Catholic Academy and must be used in accordance with this policy which adheres to the Computer Misuse Act 1990 and the Data Protection Act 1998 (see Glossary). The Academy assumes responsibility of maintenance of all hardware and software. Mis-use of equipment includes, but is not limited to the following:

- Modification or removal of software
- Unauthorised configuration changes
- Creation or uploading or computer viruses or other malware

- Deliberate deletion of files.
- The uploading of computer files to the Academy's network

Any of these actions reduces the availability and reliability of computer equipment, puts other users' data at risk and increases downtime caused by repairs, thus delaying other essential work such as upgrades or enhancements.

1.2 Laptop Computers

Laptop computers are issued to all teaching staff and support staff as required. Laptops remain the property of Saint Martin's Catholic Academy all times, and their usage is subject to the following guidelines:

- The equipment remains the property of Saint Martin's Catholic Academy at all times and must be returned to the Academy at the end of the lease agreement or contractual period.
- Maintenance of the equipment is the responsibility of the Saint Martin's Catholic Academy. All maintenance issues must be referred to the ICT Technician, through the usual channels.
- All installed software MUST be covered by a valid license agreement held by *Saint Martin's Catholic Academy*.
- All software installation MUST be carried out by the ICT Technician in accordance with the relevant license agreements.
- No software should be removed, uninstalled or disabled under any circumstances. Any software problems should be reported through the usual support channels.
- Antivirus software must be updated regularly. For laptop computers, it will be necessary to connect them to the Academy network or home internet to update the antivirus software. This should be done at least weekly.
- The user of the equipment is responsible for all personal files and data stored on the equipment. Backup of the data is the responsibility of the user. It is strongly recommended that all data is regularly backed up, either to a CDRW disk, a memory stick or to the Saint Martin's Catholic Academy network. Where removable media is used the user must ensure that these mediums have not been used to download materials that are at risk of damaging the network. It is recommended that the Academy's facility to transfer files is used.
- The user of the equipment must not encrypt <u>any</u> data or password protect any files so as to ensure future usage of the equipment.
- Saint Martin's Catholic Academy cannot be held responsible for loss of data in the event of either a hardware or software failure or user error.
- From time to time, it may be necessary for the ICT Technician to perform software updates and maintenance for which the equipment must be made available in Academy when reasonably requested.

1.3 Use of Removable Storage Media

Whilst staff may use CD disks or flash memory devices to transfer files between home and Academy, Saint Martin's Catholic Academy cannot guarantee the correct operation of any removable media or the integrity of any data stored on it. It should be noted that rewriteable CDs in particular are neither robust nor reliable, and should not be used as the sole means of storage for important files. Saint Martin's Catholic Academy cannot guarantee

the correct operation of flash memory devices on the system, although every effort is made to ensure that this facility is available.

1.4 Printers and Consumables

Printers are provided across the Academy for educational or work-related use only. All printer usage can be monitored and recorded.

- Always print on a black & white printer unless colour is absolutely essential
- Proof-read your document on-screen and use the 'Print-Preview' facility to check the layout before printing.
- Do not print unnecessarily or waste ink or paper.
- Print only what you absolutely need.
- If, more than one copy of any print is needed, photocopy the original in the Reprographics office. Please see the ICT Technician or Reprographics technician about this kind of printing and photocopying options.
- Avoid printing directly from the Internet where possible. Internet pages are often not suitably formatted for printing and may cause wastage of paper and other consumables.

1.5 Data Security and Retention

All data stored on the Saint Martin's Catholic Academy network is backed up daily and backups are stored for up to at least four weeks. If you should accidentally delete a files or files in your folder or shared area, please inform the ICT 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 and Email

2.1 Content Filtering

Saint Martin's Catholic Academy provides Internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. If you discover any websites containing inappropriate or offensive content, please report these to the ICT Technician so that they can be filtered.

2.2 Acceptable use of the Internet

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

- Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws
- Only access suitable material – Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

- Respect the work and ownership rights of people outside the Academy. This includes abiding by copyright laws.
- Do not access Internet chat sites. These represent a significant security threat to the Academy's network.
- The use of online gaming sites is prohibited. These consume valuable network resources that may adversely affect the performance of the system.
- Do not print out pages directly from a website. Web pages are often not suitably formatted for printing and this may cause significant wastage of paper. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.
- Do not attempt to download or install software from the Internet. The ICT Technician assumes responsibility for all software upgrades and installations.

2.3 Email

Staff are provided with an email address by Saint Martin's Catholic Academy. This may be used for any legitimate educational or work-related activity. Staff should use the email in accordance with the following guidelines and are reminded that the Academy retains the right to monitor email communications at any time if this is deemed necessary.

The sending or receiving of messages which contain any inappropriate material is strictly forbidden. This material includes, but it not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, or any other use which may be likely to cause offence. Disciplinary action will be taken in all cases.

- Messages relating to, or in support of any illegal activities may be reported to the authorities.
- Whilst it is possible to attach files to an email message, staff are advised that that email is not generally suited to transferring large files. Whilst there are no hard and fast rules regarding file sizes that can be attached to an email message, files exceeding approximately 5MByte in size are generally considered to be excessively large and staff 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 or other forms of malware that may cause loss of data or damage to the Academy network.
- Staff should not send personally identifiable information by email, as it is not a secure medium.

3. External Services

Saint Martin's Catholic Academy provides a number of services that are accessible externally, using any computer with an Internet connection. These should be used strictly for educational or work-related activities only and in accordance with the following guidelines

3.2 Web-Email

Web email (Microsoft Office 365) 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. Staff should use email in accordance with the following guidelines and are reminded that the Academy retains the right to monitor email communications at any time if this is deemed necessary.

- Web-email (Microsoft Office 365) is provided for use of Saint Martin's Catholic Academy staff, students, governors, trainee teachers and some short-term, voluntary staff. Access by any other party is strictly prohibited.

- By using Web-Email (Microsoft Office 365), you signify that you are an employee or volunteer at Saint Martin's Catholic Academy, and that you have been authorised to use the system by the relevant Academy authority.

- Observe security guidelines at all times. Never reveal your password to anyone

- Remember to treat file attachments with caution. File attachments may contain viruses or other forms of malware 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. If you are not sure if the email message containing a link to an unknown web site or attachment file (.pdf, word, excel, .html, .htm, .vbs, .bat) please inform the ICT technician as soon as possible without clicking any of the links or opening any of the attached documents. Saint Martin's Catholic Academy accepts no responsibility for damage caused to any external equipment or software as a result of using the web-email service.

- The rules that apply to Email are also to Web-Email.

3.3 Microsoft Teams

St Martin's MS Teams sites are provided for use in relation to Academy activity e.g. collaboration and communication relating to: academic study; engagement in Academy-led clubs, events and activities. Guest access can be arranged for third parties working outside of the Academy.

MS Teams is an Office 365 cloud service and therefore information contained within our Academy Teams sites is stored in Microsoft Data Centres. This meets UK and EU data protection and security standards.

It is important that users recognise that this is an Academy provisioned service and therefore users must adhere to the guidance below or risk disciplinary action.

- Use your own name and photograph within your Office 365 profile. It is important that members are clear about who they are interacting with.

- MS Teams is designed to support professional networks, therefore, do not over disclose personal information and protect yourself against identity theft.

- MS Teams sites are created for use by student and staff members, however, as these are Academy own sites they may be accessed and monitored by Academy staff members who are not visible members of your MS Team. An example of this may be the monitoring of particular key terms as part of activities undertaken by the Academy to safeguard our student and staff environment and provide an inclusive place to study and work.

- All MS Teams channels and discussions are visible to all members of the MS Team site. Private messaging is available to send direct messages to selected members.

- Treat team members with respect. It is important that this is maintained throughout even in instances when opinions differ. Be clear and avoid using ambiguous language which may be open to misinterpretation.

- Make sure you clearly understand the purpose of your MS Teams site. Stay on topic and avoid sharing irrelevant content as this may frustrate other members. No spam.

- MS Teams provides a file storage location for files posted within conversations and channels. This provides a time limited repository and should not be used as a substitute for personal storage solutions such as OneDrive; staff and student home folders or departmental files storage. St Martin's Catholic Academy and Microsoft cannot guarantee that we can retrieve data previously saved in this location after the MS Team site is closed.

- You should ensure that the sharing of images and videos does not breach image rights and copyrights. Seek permission from anyone included in personal photographs prior to sharing them.

- In most instances there is no need to share Confidential or Personal or Sensitive information via MS Teams and this should be discouraged within the MS Teams site. Individuals Personal and Personal Sensitive information must not be requested or shared. Sharing your own data should only be done when there is a valid reason and done so at your own risk. Where there is a need to share Confidential information, this should be labelled as 'Confidential'; appropriate permissions should have been sought from the data owner prior to sharing; the purpose of sharing the data should be transparent to the group and there should be a clear timeframe set to ensure that this data is removed as soon as it is no longer needed. The sharing of Confidential, Personal and Sensitive information increases the risk of data breaches and when breaches occur this may result in disciplinary action taken against the individual sharing the data and action against the St Martin's Catholic Academy by data protection regulators.

- Information shared within your MS Teams site is for use by your site members only (Staff; Students or external Guests) and should not be shared outside of the MS Teams site without appropriate permissions. No Confidential, Personal or Sensitive information should be shared outside of your MS Teams site or the Academy.

- St Martin's Catholic Academy reserves the right to remove inappropriate MS Teams sites or posts. This may include posts that damage the reputation of individuals or the Academy, include defamatory comments that cause distress to members of our Academy community, that contain obscene content or breach civil or criminal law. If you post inappropriately and later remove this post this may still be accessed by the Academy and used within disciplinary procedures as appropriate. Typically, a MS Teams site will have two nominated site owners who will monitor use and ensure inappropriate posts are removed. Such posts may lead to disciplinary action.

3.4 Microsoft One Drive Cloud Storage

OneDrive is the Microsoft cloud service that connects you to all your files. It lets you store and protect your files, share them with others, and get to them from anywhere on all your devices. You can access OneDrive cloud storage services logging on to Microsoft Office 365 online services using your email and password (https://www.office.com) or opening the OneDrive application on your computer and logging onto it using your Academy provided email account.

All files that you store in OneDrive are private unless you decide to share them. You can share files and folders with co-workers so you can collaborate on projects. If you're signed-in to Microsoft Office 365, you may even be able to share with partners outside of your organization, depending on what St Martin's Catholic Academy allows. Microsoft will store data uploaded by staff accounts in EEA or US Safe Harbour locations. For more info about the ownership of your data, see Office 365 Privacy by Design.

Using One Drive for work or school via a staff logon ID is therefore the recommended Cloud Storage solution for use by Academy staff.

Our current Microsoft 365 licence gives all staff and students up to 1TB storage space each!

Please observe these rules when you are using One drive cloud storage:

- Do not use cloud storage to store files containing information about individuals or other sensitive information.

- Do not use cloud storage for the long-term retention of Academy documents or files even for instances when you work with non-sensitive information. Use alternatives such as SharePoint and shared network drives.

- If you are using Cloud Storage for collaboration with others, either from within the Academy or elsewhere, only grant access to files or folders that are required for the collaboration to take place. Access to personal data should be given on a strictly need to know basis to comply with the Data Protection Act.
- St Martin's Catholic Academy does not support cloud storage clients or apps, such as those available for Dropbox.
- Do not store the only copy of a file in cloud storage.
- You must ensure that there is a suitable level of encryption on any mobile or portable device used to download any data about individuals from cloud storage. Such a device must be password protected.
- Only store work related files and documents in cloud storage.

4.0 Privacy and Data Protection

4.1 Passwords

- Never reveal your password to 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. It is advisable to use a 'strong' password. A strong password is one which contains a combination of upper and lower-case letters, numbers and other punctuation characters. You can substitute numbers and letters for other characters that look similar, such as '3' for 'E', '1' for 'I' or '@' for 'O', '!' for '1' etc. This will help to make your password much more difficult to guess. Remember that passwords are case-sensitive.
- If you forget your computer login password or email password, please contact the ICT Technician for a password reset process.
- If you believe that a student or other staff may have discovered your password, then change it ***immediately***.

4.2 Security

- Never attempt to access files or programs to which you have not been granted authorisation. 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 the ICT Technician.
- Any user identified as a security risk will be denied access to the system and subject to disciplinary action in accordance with the Academies Disciplinary Procedures.

5.0 Management and Information Systems

Access to MIS software is available from designated STAFF computers and only to those staff who require it. Access is subject to agreement with the Operations Manager. Usage of MIS software is subject to the following guidelines:

- Password security is vital. If you believe that your password has been discovered by a student or other member of staff, **change it immediately**.

- If you leave your computer unattended, particularly in a classroom, either log out or lock it by using the CTRL-ALT-Delete keys and then choosing "Lock". Once this is done, you will need to re-enter your password to gain access to the computer.

- If you are using MIS software on a computer in a classroom connected to an interactive whiteboard and projector, please be aware that any student information you display on your screen may also be displayed on the whiteboard if the projector is turned on. To ensure protection of sensitive data, please ensure that projectors are turned off or disconnected before using MIS software.

- Within Saint Martin's Catholic Academy it is understood that the Headteacher and Senior Leadership team have a clear duty of care to protect the access to confidential data. Further details regarding this aspect of the Academy's E-safety approach can be found in Appendix G (Management and Information Systems).

- Where staff are working at home and connect remotely to the Academy's computer network and MIS system then all of the above considerations also apply. Staff must ensure that their home Internet connection is secure from outside access particularly if a wireless network is used. Additionally, staff should take due care of any material which they print at home.

6.0 Mobile Technologies

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

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 live video streaming and downloadable video clips from films, sporting events, music and games etc. The capabilities of 3G, 4G and 5G mobile phones also means that adults working within the Academy environment may be sent inappropriate images or videos, or be encouraged to send back images or video of themselves using integrated cameras.

In order to reduce the opportunity for those behaviours that could possibly cause upset, it is advisable that staff, governors and volunteers working with children and young people within the Academy setting, limit their use of mobile technologies to necessary communication during specified breaks during the Academy day.

If you are sent inappropriate material e.g. images or videos **report it immediately**.

7.0 Support Services

All ICT hardware and software maintenance and support requests should be submitted to the ICT Technician using one of the following methods:

- Email support@saint-martins.net or vozkan@saint-martins.net
- By dialling internal extension number 221 or the school phone number from outside (01455 212 386).
- In person at the ICT Technician's Room.
- By leaving a message at reception for the ICT Technician.

Saint Martin's Catholic Academy will make every effort to ensure that all technical or operational problems are resolved within a reasonable time.

7.1 Software Installation

The ICT Technician assumes responsibility for all software installation and upgrades. Staff may request the installation of new software packages onto the network, but this will be subject to the following:

- A minimum of 3 working days is required for packaging and installation of new software.
- Software cannot be installed on the Academy's network without a valid license agreement. This must be supplied with the software package.
- Please check the licensing terms of the software package carefully to ensure that it is suitable for use on the Academy network. If you are unsure, please ask the ICT Technician for assistance or contact the software supplier. A relevant and valid license agreement document will be required before any software packages can be installed.
- All software installation media and license agreements are held centrally within the Academy to aid in license tracking and auditing. Installation media cannot normally be released except by special agreement.
- When purchasing new software for use on the Academy network, please check its suitability, compatibility and licensing terms with the ICT Technician. Purchase orders for new software will normally be authorised only with the agreement of the Head of Department/budget holder.

7.2 Service Availability

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the Academy 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 Academy ICT system is at your own risk. Saint Martin's Catholic Academy specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

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 another user's password and use it.
  - Unauthorised access to deliberately commit an unlawful act e.g. if you guess another user'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 Academy'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 Academy.

  The Act covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in the Academy. 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 protection

- RIPA – Regulation of Investigatory Powers Act 2002
  If a request for authorised access is made to the Academy 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 Academy, we will provide the appropriate access to your ICT records and files.

DECLARATION

MEMBER OF STAFF/VOLUNTEER

I understand and agree to the provisions and conditions of this, Authorised Acceptable Use, agreement.

I understand that any violations of the outlined provision may result in disciplinary action and revocation of privileges.

I also agree to report any misuse of the system to the ICT Technician.

I agree to use the Internet and electronic communications systems in compliance with the terms outlined in this document and understand that my Internet access and any electronic communications may be logged or monitored.

NAME _____

SIGNATURE _____

DATE _____