St Mary Magdalene Academy
The Courtyard

THE COURTYARD

ACCEPTABLE USE OF ICT POLICY

The Courtyard aims to offer an outstanding educational and social provision that will equip our pupils with the skills and experiences needed to discover and live out their potential.

ACCEPTABLE USE OF ICT - POLICY STATEMENT

ST MARY MAGDALENE ACADEMY
THE COURTYARD

Approval Committee:	**Full Governing Body**
Author:	**Head of The Courtyard**
Last reviewed:	**March 2022**
Next review date:	**March 2023**
Required to publish on website?	**No**
Statutory?	**No**

Key Points of our Acceptable Use Policy for Adults

SMMA: The Courtyard has provided computers for use by staff as an important tool for teaching, learning and administration of the school. Use of school computers, by both members of staff and pupils, is governed at all times by the following policy. Please ensure that you understand your responsibilities under this policy, and direct any questions or concerns to the Headteacher or ICT Network Manager in the first instance.

The purpose of the policy is to ensure the school network is operated safely and all users of ICT are safe. It refers to our school ICT network and to the use of mobile technologies within it and explains the behaviours, which are acceptable and unacceptable within our school.

This document outlines the key points of our Acceptable Use of ICT Policy ('AUP'). It has been written to ensure all adults working within school are aware of the rules, risks and procedures we operate under our full AUP, which is located on our ICT system.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Our AUP must be fully complied with at all times. All users of the school network should note that it is monitored on a regular basis. Any person who is found to have misused the school system or not followed our AUP could face the following consequences:

- Temporary or permanent withdrawal from the school system
- Suspension or exclusion from the school
- Disciplinary action
- In the most serious cases legal action may also be taken.

Whilst our network and systems are organised to maintain the most secure environment possible **it is every adult's responsibility to make sure the pupils you are directly working with are safe**. All adults working in school must do so under the guidance of the member of staff to whom they are responsible.

As an adult working in school you may be the first point of contact in dealing with incidents of ICT misuse or abuse. Every such incident must be reported to the Headteacher who will then follow the procedures set out in our AUP.

Your key responsibilities are:

- Maintaining an appropriate level of professional conduct in your own internet use within school.
- Developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children.
- Implementing our school AUP through effective classroom practice.
- Reporting any instances of ICT misuse to the Headteacher who must report it to the ICT Network Manager in line with our school AUP. If the Headteacher is suspected of being involved, report directly to the ICT Network Manager or the Chair of Governors (Eliot.Brooks@smmathecourtyard.org)

- Supporting pupils who experience problems when using the internet.
- Using the internet and ICT facilities to ensure that internet safety is not compromised e.g. evaluating websites in advance of classroom use, using child oriented search engines.
- Embedding internet safety messages wherever possible.
- Following the school rules relating to acceptable use of our ICT equipment and other mobile technologies.
- Copies of our rules for pupil use of the network are displayed around the school. Please ensure you have read them and make sure the pupils you work with adhere to them.

School ICT Network

The school network and associated services may be used for lawful purposes only.

Passwords

- Each pupil and adult working within the school must log on to the computers using the username and password given to them. Passwords need to be kept a secret. If for any reason a pupil or adult needs to leave their computer, they have to lock the computer to prevent others from using their account by pressing 'Ctrl, Alt and Delete'.
- It is forbidden to use other pupils/adult's accounts or files. Both adults and pupils will respect copyright and not copy anyone's work and call it their own.
  For the pupils in our school who are unable to understand the 'Pupils Acceptable Usage Policy' and for the pupils who are unable to log in and log off using their own password, the adult(s) working with those pupils will take full responsibility for their safe internet use in school.

Software and Downloads

- All users of the network must virus check any USB device storage devices before using them on the network.
  All users are prohibited from installing software onto the network from a CD-ROM, other device or by downloading from the Internet without permission from the ICT Technician. If users need a new program installing onto the computer, our ICT Technician will be asked to do this if possible.
- Copyright and intellectual property rights must be respected when downloading from the internet.

Personal Use

The school recognises that occasional personal use of the school's computer by members of staff is beneficial both to the development of ICT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

- Most comply with all other conditions of the AUP as they apply to non-personal use, and all other school policies regarding staff conduct.

- Must not interfere in any way with your other duties or those of any other member of staff.
- Must not have any undue effect on the performance of the computer system; and
- Must not be for any commercial purpose or gain unless explicitly authorised by the school.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

Email

- All members of staff with a computer account in school are provided with a school email address for communication both internally and with other email users outside of school.
- No member of staff (including governors and non-teaching staff) must use non-school email accounts for any school/work related activity – no exceptions!
- Members of staff are responsible for e-mails they send and should be aware that these are open to be read and should be treated as public.
- Users should be aware that email is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
- E-mails should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Anonymous messages and chain letters must not be sent.
- When writing emails, you should use appropriate language. You should not use language that could be calculated to incite hatred against ethnic, religious or other minority or any other protected group. You need to remember that you are a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- All emails both sent and received will be scanned by forensic software.
- E-mail attachments should only be opened if the source is known and trusted.
- Pupils are not permitted under any circumstances to e-mail a member of staff using their personal e-mail address. In addition, members of staff should not be emailing pupils using their personal email address.
- Privacy –personal information (e.g. name, address, age, telephone number, social network details) of other users should not be revealed to any unauthorised person. Users should not reveal any of their personal information to the pupils.
- Users will not trespass into other users' files or folders.
- Users will ensure that all login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual other than myself. Likewise, Users will not share those of other users. Users will ensure that if they think someone has learned their password then they will change it immediately and/or contact ICT technician.

- Users will ensure that they log off after their session has finished. If they find an unattended machine logged on under another username they will not continue using the machine – they will log it off immediately.
- Any unsuitable communications received must be reported to a member of staff immediately.

Images/Videos

- All pupils need parental permission to have photographs or videos published electronically or in a public area even if they are unidentifiable.
- No photos or videos which include nudity or inappropriate actions are permitted to be taken or downloaded under any circumstance.

Network Protocol

- School computer and Internet use must be appropriate to a pupil's education or to staff professional activity.
- Respect other people's material and do not corrupt, interfere with or destroy it
- Do not open other people's files without expressed permission.
- When working with personal data ensure that the data is secure.

Internet Usage

- Pupils must be supervised at all times when using the internet.
- Activities should be planned so 'open searching' is kept to a minimum. The facility for caching sites should be used prior to using the internet with pupils.
- When searching the internet with pupils, members of staff should encourage the pupils to use 'young person safe' search engines. However safe search is set on all computers in school as a default on search engines.
- The use of social networking sites, public chat rooms and messaging systems (e.g. Facebook, Messenger, Twitter) is not allowed in school.
- Use the internet for personal financial gain, gambling, political purposes or advertising is forbidden.
- Users will not attempt to visit websites that may be considered inappropriate or illegal. Users are aware that downloading some material is illegal and that the police or other authorities may be called to investigate.
- Users must never open emails from unknown senders. They should always consider whether this could contain a virus and refer to the Headteacher if they have a concern.

Use of Social Networking Sites and Online Forums

Staff must take care when using websites such as Facebook, Twitter, Dating Sites etc, even when such use occurs in their own time on their own computer at home. Social Networking sites invite users to participate in informal ways that can leave them open to abuse, and often make little or no distinction between adult users and children / young people.

Users must not allow any pupil to access personal information they post on a social networking site. In particular:

- Users must not add a pupil to your 'friends list', nor invite them to be friends, even if the pupil issues an invite.
- Users must ensure that personal information is not accessible via 'Public' setting, but ensure it is to a 'Friends only' level of visibility.
- Users should avoid contacting any pupil privately via social networking site, even for school-related purposes.
- Users should take steps to ensure that any person contacting them via a social networking website is who they claim to be, and not an imposter, before allowing them to access personal information.

It is advised not to accept invitations from the pupils' parents or carers on social networking sites, nor should Users invite them to be friends. As damage to professional reputations can inadvertently be caused by quite innocent postings or images. Users will need to ensure that any private social networking sites/blogs that they create or actively contribute to are not to be confused with their professional role in anyway.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, users must not post comments on websites that may appear as if they are speaking for the school.
- Users should not post any material online that can be clearly linked to the school that may damage the school's reputation.
- Users should avoid posting any material clearly identifying themselves, another member of staff, or a pupil, that could potentially be used to embarrass, harass or defame the subject.

Use of your own Equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and must not be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing.
- Users must not connect personal computer equipment to school computer equipment without prior approval from ICT Technician, with the exception of storage devices such as USB memory sticks, but only post checking the USB is virus free.

Mobile Devices

- Personal mobile phones should not be used in areas of school where pupils have access.
- During teaching time, mobile phones should be turned off or put on silent mode and stored away from pupils.

- Adult are allowed to access their personal phones on breaks, lunch times and after school.

Supervision of Pupil Use

- Pupils must be supervised at all times when using school computer equipment. When arranging use of computer facilities for pupils, you must ensure supervision is available.
- Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.
- Supervising staff must ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.

Reporting Problems with the Computer System

It is the job of the ICT Network Manager to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible.

- Users should report any problems that need attention to ICT Technician.
- If Users suspect their computer has been affected by a virus or other malware, they must report this to ICT Technician immediately.
- If Users have lost documents or files, they should report this as soon as possible. The longer a data loss problem goes unreported, the less chances of the data being recoverable.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. Users must immediately inform the ICT Technician or the Headteacher, of abuse of any part of the computer system. In particular, Users should report:

- Any websites accessible from within school that they feel are unsuitable for staff or pupil consumption.
- Any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc.
- Any breaches, or attempted breaches, of computer security, or
- Any instance of bullying or harassment suffered by Users, another member of staff, or a pupil via the school computer system.

All reports will be treated confidentially.

Electronic Devices - Searching & Deletion

In accordance with ‘The Education Act 2012’ the Headteacher of the Courtyard School has the right to search and or delete anything from personal devices of staff if they believe illegal or suspicious activity is taking place.

Using Your Own Device

When a User uses his or her own device, the School is exposed to a number of risks, including the loss or theft of the device (which could result in unauthorised access to our systems or school data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device) and the loss or unauthorised alteration of school data (including personal and confidential information which could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy). Such risks could result in damage to the School and its reputation.

For the avoidance of doubt, the sections of this IT Acceptable Use Policy on proper use of the school technology system, transmitting improper or unlawful material, cautious use of the internet, copyright laws and software licences, no expectation of privacy, monitoring, protecting confidential information and password security apply whether or not the User is accessing the School system via a School owned device or a personally owned device.

The Courtyard's policy on Security Incident Reporting of any confirmed or suspected security incidents also applies to any personal device which is being used for work purposes and must be reported to the Headteacher or Data Protection Officer immediately.

Users are expected to have taken all reasonable steps to ensure that anti-virus, anti-malware software is installed, that their device is password protected and its operating system is current with any critical security patches or updates.

The School IT Service Desk will not be responsible for troubleshooting connectivity issues with personal mobile phones, Laptops, Mac's, or tablets or wifi Access.

Users are permitted to use personal devices for work purposes where authorised by the School. Users are not authorised to connect their personal mobile phone, laptop, or tablet to the School Wifi.

Access to School Data

Users are not permitted in any way to transfer school data of any kind from the school shared networks to their personal devices. This includes finance, pupil, staff and partner school data.

Remote Access to G-Drive

This can be done via the Googledrive App.

Exemptions

All the above stands unless given permission from the Headteacher e.g. while on residential trips, permission may be given to designated staff to upload photos onto the school website.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

Our Acceptable Use Policy (AUP) has been created by the Headteacher and approved by governors and the whole school community.

I have read, understood and agree to comply with the AUP:

Signed: _____ Date: _____

Print Name: _____

Position in School: _____