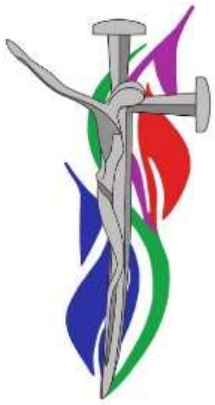

Achieving together in faith

Holy Cross Catholic MAC

ICT and Internet Acceptable Use Policy
2022 / 2024

Responsible for policy	Christopher Connoll
Date of policy	February 2022
Date approved by HCC MAC Board	16 February 2022
Date of policy review	February 2024

Document Control:

Version History

Version	Status	Date	Author	Department	Summary of Changes
1.0	Draft	05/2021	J Parry	HCCMAC, Central Team	Creation of document from template
1.1	Draft	06/2021	C Connoll	HCCMAC, Central Team	
1.1	Draft	12/2021	C Connoll	HCCMAC, Central Team	Share with ITSWG Approved by Directors with changes to Section 5.2
2.0	Draft	03/2022	C Connoll	HCCMAC, Central Team	Changes made to Section 5.2 and appendix
3.0	Draft	03/2022	C Connoll	HCCMAC, Central Team	Further updates to Section 5.2 and appendix

Contents

1. Introduction and aims

ICT is an integral part of the way our organisation work, and is a critical resource for pupils, staff, Directors, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of Holy Cross Catholic Multi Academy Company (MAC).

However, the ICT resources and facilities that are used also pose risks to data protection, online safety and safeguarding and cyber security.

This policy aims to:

- Set guidelines and rules on the use of ICT resources.
- Establish clear expectations for the way all members of the MAC community engage with each other online.
- Support the MAC's policy on data protection, online safety and safeguarding.
- Prevent disruption to the MAC through the misuse, or attempted misuse, of ICT systems.
- Support schools in teaching pupils safe and effective internet and ICT use

This policy covers all users of the MAC's ICT facilities, including Directors, governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under the MAC's Codes of Conduct.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2020
- Searching, screening and confiscation: advice for schools

3. Definitions

- **“MAC ICT facilities”:** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **“Users”:** anyone authorised by the MAC to use the ICT facilities, including Directors, governors, school staff, pupils, volunteers, contractors and visitors
- **“Personal use”:** any use or activity not directly related to the users’ employment, study or purpose
- **“Authorised personnel”:** employees authorised by the MAC to perform systems administration and/or monitoring of the ICT facilities
- **“Materials”:** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the MAC's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the MAC's ICT facilities includes:

- Using the MAC's ICT facilities to breach intellectual property rights or copyright
- Using the MAC's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the MAC's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the MAC/schools, or risks bringing the MAC/schools into disrepute
- Sharing confidential information about the MAC/schools, its pupils, or other members of the MAC/school community
- Connecting any device to the MAC/school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the MAC/school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the MAC/school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Catholic Senior Executive Leader (CSEL), headteacher or any other relevant member of staff, will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of MAC school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the CSEL's/headteacher's discretion. Approval should be sought from the CSEL/headteacher prior to such activities being undertaken.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the MAC/school's policies and Codes of Conduct, copies of which may be found on the MAC website www.hcmac.co.uk

5. Staff (including Directors, governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The MAC ITCC Manager / School ICT Provider / Business and/or Office Manager manages access to ICT facilities and materials for school staff. This includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the MAC/school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT Manager/ School ICT Provider/ Business/ Office Manager.

5.1.1 Use of phones and email

Each member of staff is provided with an email address if their role requires access to emails. This email account should be used for work purposes only.

All work-related business should be conducted using the email system and address the MAC/school has provided.

Staff must not share their personal email addresses with parents or pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the MAC ITCC Manager / Business/Office Manager / Headteacher immediately and follow the data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must only use phones provided by the school to conduct all work-related business. School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Staff who would like to record a phone conversation should speak to their MAC ITCC Manager/ Business/Office Manager All non-standard recordings of phone conversations must be pre-approved, and consent obtained from all parties involved.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. ICT equipment should not be used for own use/personal use during non-break times and permission may be withdrawn or restricted at any time at the discretion of the MAC ITCC Manager / CSEL / Headteacher. Personal use is permitted provided that such use:

- Does not take place during non-break time.
- Does not constitute 'unacceptable use', as defined in section 4.
- Takes place when no pupils are present.
- Does not interfere with their jobs or prevent other staff or pupils from using the facilities for work or educational purposes.

Staff may not use the MAC/school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the MAC/school's ICT facilities for personal use may put personal communications within the scope of the MAC/school's ICT monitoring activities (see section 5.5). Where breaches are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with 5.2 above.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The MAC school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely in line with the MAC's Remote Learning Policy.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take precautions against importing viruses or compromising system security.

MAC/school ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with the MAC's Data Protection Policy which is available on the MAC website.

5.4 MAC/School social media accounts

The MAC/schools have official Facebook/Twitter/etc. pages, managed by MAC/school staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The MAC/school has guidelines for what can and cannot be posted on social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Monitoring of school network and use of ICT facilities

The MAC/school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications
- Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The MAC/school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Pupils

6.1 Access to ICT facilities

- Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff (unless permission has been given, secondary only)
- Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff (unless permission has been given, secondary only)
- Secondary School Pupils will be provided with an account linked to the school's virtual learning environment, which they can access from any device
- Sixth-form pupils can use the computers independently for educational purposes only
- Primary School Pupils must only access technology under the supervision of staff.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, schools have the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under MAC/school rules or legislation.

The MAC/school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the MAC/school's rules.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils if they engage in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright.
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the MAC/school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the MAC/school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, other pupils, or other members of the MAC/school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the MAC/school's ICT facilities.
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the MAC/school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

8. Data security / Encryption

The MAC/school takes steps to protect the security of its computing resources, data and user accounts. However, security cannot be guaranteed. Staff, pupils, parents and others who use the MAC/school's ICT facilities should use safe computing practices at all times. The MAC/school ensures that its devices and systems have an appropriate level of encryption.

Staff may only use personal devices to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the CSEL/headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption.

USB Storage devices are not to be used as these are block by the Information Security Policy to protect our data.

8.1 Passwords

All users of the MAC/school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Anyone disclosing account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

All of the MAC/school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the MAC/school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the MAC's data protection policy which is available on the MAC website at hccmac.co.uk.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the ICT/Business/Office Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

9. Internet access

MAC and school wireless internet connections are secured.

9.1 Pupils

Where the school allows, access to Wi-Fi is to be used for education purposes only and will be kept secure and will be filtered according to the user type. Pupil access to Wi-Fi is limited to post 16 pupils only unless access is granted by the School IT Manager, Headteacher and/or MAC ITCC Manager.

9.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's Wi-Fi to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Monitoring and review

The CSEL, MAC ITCC Manager, headteacher and ICT/Business/Office Manager monitor the implementation of this policy including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every two years.

11. Related policies

This policy should be read alongside the MAC/school's policies on:

- Information Security
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote learning

Appendix 1: Social Media advice sheet

Don’t accept friend requests from pupils on social media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don’t share anything publicly that you wouldn’t be just as happy showing your pupils
6. Don’t use social media sites during work hours (unless part of your job)
7. Don’t make comments about your job, your colleagues, your MAC/school or your pupils online – once it’s out there, it’s out there
8. Don’t associate yourself with the MAC/school on your profile (e.g. by setting it as your workplace, or by ‘checking in’ at a school event)
9. Don’t link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information

---

Check your privacy settings

- Change the visibility of your posts and photos to **‘Friends only’**, rather than ‘Friends of friends’. Otherwise, pupils and their families may still be able to read your posts, see things you’ve shared and look at your pictures if they’re friends with anybody on your contacts list
- Don’t forget to check your **old posts and photos**
- The public may still be able to see posts you’ve **‘liked’**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile.
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
  - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to the Social Media Platform or the relevant social network and ask them to remove it
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police