Acceptable Use Policy

Responsible for policy	CC3 Quality, Provision, Performance and Standards
Date of policy	April 2020
Date reviewed by CC3	June 2022
Date of review	September 2024
Chair of Directors	Brendan Fawcett

Contents

Definitions

In this **Acceptable Use Policy**, unless the context otherwise requires, the following expressions shall have the following meanings:

i ‘**The Romero Catholic Academy**’ means the Company named at the beginning of this **Acceptable Use Policy** and includes all sites upon which the Company is undertaking, from time to time, being carried out. The Romero Catholic Academy includes; **Corpus Christi**, **Good Shepherd**, **Sacred Heart**, **Blue Sky**, **SS Peter and Paul**, **St Gregory**, **St John Fisher**, **St Patrick**, **Cardinal Wiseman**, **Shared Services Term**.

ii ‘**Romero Catholic Academy’** means the Company responsible for the management of the Academy and, for all purposes, means the employer of staff at the Company.

iii ‘**Board’** means the board of Directors of the Romero Catholic Academy.

iv ‘**Governance Professional’** means the Governance Professional to the Board or the Governance Professional to the Local Governing Body of the Academy appointed from time to time, as appropriate.

v ‘**Chair’** means the Chair of the Board of the Directors or the Local Governing Body appointed from time to time.

vi ‘**Catholic Senior Executive Leader**’ means the person responsible for performance of all Academies and Staff within the Multi Academy Company and is accountable to the Board of Directors.

vii ‘**Diocesan Schools Commission**’ means the education service provided by the diocese, which may also be known, or referred to, as the Birmingham Diocesan Education Service.

viii ‘**Local Governing Body’** means the governing body of the School.

ix ‘**Governing Body Representatives’** means the governors appointed and elected to the Local Governing Body of the School, from time to time.`

x ‘**Principal’** means the substantive Principal, who is the person with overall responsibility for the day to day management of the school.

xi ‘**School’** means the school or college within The Romero Catholic Academy and includes all sites upon which the school undertaking is, from time to time, being carried out.

xii ‘**Shared Services Team’** means the staff who work in the central team across the Company (e.g. HR/ Finance)

xiii ‘**Vice**-**Chair’** means the Vice-Chair of the Governing Body elected from time to time.

xiv **‘Academy Head of IT’** means the person responsible for IT across the Academy

xv **‘IT Team’** means the team of staff supporting the Academy Head of IT and the individual academies

1. Overview

The Acceptable Use Policy (AUP) is set in place to uphold the integrity of IT systems at The Romero Catholic Academy in terms of maintaining an ethos of honesty, trust and collaboration. The Romero Catholic Academy is committed to protecting all stakeholders from illegal or inappropriate activities that may be perpetrated by individuals with or without their knowledge.

IT systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing E-mail and Internet browsing are the property of The Romero Catholic Academy. These systems are to be used for purpose of education in terms of the primary business activity of the organisation. Stakeholders of the system in this instance include: Pupils and authorised student visitors.

Effective security is team work involving all stakeholders who access the schools information systems and associated infrastructure. It is deemed the responsibility of all system users to read and follow the guidelines of the AUP and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline acceptable use of the computer system at The Romero Catholic Academy. These procedures are in place to protect pupils and all stakeholders from inappropriate activities that might compromise the IT infrastructure and reputation of The Romero Catholic Academy.

All stakeholders are required to accept procedures and practices that safeguard the security, integrity and safety of information created and held by The Romero Catholic Academy through the adherence of the AUP.

3. Scope

This Policy applies to all stakeholders authorised to have access to the Academy's IT Services and facilities. This Policy applies to all Academy IT services and property, whether they are located on or off site.

For the purpose of this Policy, The Romero Catholic Academy IT Services facilities contain all:

- Physical or virtual computers to include: Servers, desktops, terminals or mobile devices.
- Peripherals such as: Monitors, keyboards and printers
- Computer networks, including wireless and IP Telephony networks
- Software and data held within the IT infrastructure.
- Computer-based information systems provided for education and administration.
- Devices not owned by The Romero Catholic Academy are connected to the Academy network and its services.
- AUP Pupils/Student Visitors

Summary

Your checklist

Review
Review the privacy settings for your social media, professional networking sites and app accounts.

Know
Know who to report any unusual activity to. If you're not sure, ask your line manager or IT team.

Check
Check your device is set to receive updates automatically.

Set
Set a strong password and switch on two-factor authentication, if available, for your most important accounts.

Remove
Remove any apps that have not been downloaded from official stores.

Check
Check that the password for your work account is unique.

Flag it
If it's not possible to follow security advice, process or policy - flag it to your IT team.

4. Policy

By signing this Acceptable Use Agreement Form you are agreeing to the following guidelines. Acceptable Use forms can be found in **Appendix 1.** When using the Academy's computer systems, you should comply with the following guidelines. These guidelines are intended to help you make the best use of the computer resources at your disposal

Use of School Computer Equipment

Do

- ✓ Agree to the terms and conditions of all license agreements relating to installed software or software accessed through the school network including all restrictions related to commercial use.
- ✓ Seek authorisation to access, change, save or copy records/files and computer records.
- ✓ Conform to the AUP while using the academy's network.
- ✓ Ensure that you log out of School systems at the end of each session.
- ✓ Protect equipment from theft.
- ✓ Refrain from eating and drinking in computer suites and while accessing school equipment.
- ✓ Respect all elements of the IT environment and its infrastructure.
- ✓ Report all incidences of malicious damage to appropriate teaching staff or IT services.
- ✓ Report all incidence of hardware/software failure to appropriate teaching staff or IT services.

Do Not

- ✗ Move static computer equipment from room to room without approval from IT Services
- ✗ Install unlicensed software or applications on school computers, server's laptops or mobile devices.
- ✗ Connect phones to an academy device without the consent of the IT Services
- ✗ Install or use any device or software on the school computer system that bypasses security controls including monitoring and filtering
- ✗ Bypass any security measures used to safeguard the safe processing of information on any school computing equipment, information systems or communication equipment.
- ✗ Remove/disable of anti-virus software and password protection is prohibited.
- ✗ Produce, access, transfer or download inappropriate or extremist materials, using the Academy's IT systems or network.
- ✗ Participate in harassing, slandering or other anti-social behaviours online.
- ✗ Create or spread any offensive, obscene or rude images, data or other material in any form.
- ✗ Use the computer system to attack or gain unauthorised access to other networks, computer systems or data.
- ✗ Invade the copyright of another person or organisation
- ✗ Leave computers screens locked for more than 20 minutes, thus stopping others from using the shared resource.
- ✗ Use shareware or similar software downloaded from the Internet.
- ✗ Duplicate or copy software.
- ✗ Install any software on your machine or alter its configuration, this activity may only be undertaken by the IT Services.
- ✗ Vandalise or destroy data of a different user, the operation of the network, Internet, or other network that are connected to the Internet
- ✗ Deliberately damage computer hardware such as monitors, base units, printers, keyboards, mice, mobile devices or other hardware
- ✗ Attempt to bypass any of the Academy's security and filtering systems or download any unauthorised software or applications.
- ✗ Interfere with peripheral computer systems or devices (e.g. printers and projectors) and their cabling, internal parts or casings.

The Academy has a legal obligation to take steps to prevent individuals being drawn into extremism and terrorism, and a duty to alert and report any attempted access to, or distribution of, such unsuitable material.

5. Use of Passwords and Access

If you are unable to access your account or for any reason are unable to access services related to password protected systems contact the IT Team **using the IT helpdesk**

Do

- ✓ Change the default password given to you when you connect to the network, application or system for the first time.
- ✓ Have a password with at least eight characters long.
- ✓ Have a password with at least three of the four available character types: lowercase letters, uppercase letters, numbers and symbols.
- ✓ Consider using a passphrase instead of a password.
- ✓ Choose a password that would be hard to guess.
- ✓ Log off from your computer at the end of every session.
- ✓ Regularly change your password.
- ✓ Check emails for phishing activities that ask you to reveal your password.
- ✓ Report any suspected password compromise instantly to IT Services, and password should be changed quickly.
- ✓ Follow good security practices when choosing, using and protecting your passwords. IT Services can reset your password if required. We will never ask you to reveal your password

Do Not

- ✗ Write your password down or store it in an insecure manner.
- ✗ Use another person's username.
- ✗ Permit or allow another person to use your username/password.
- ✗ Allow your password to become known by another users.
- ✗ Disclose your account password to others or permit use of your account by others.
- ✗ Reveal your password to someone unauthorised in order to gain access to our computer system.
- ✗ Have a password that contain the username or parts of the user’s full name, such as a first name.

Your Username and password are the key device for access to the Academy’s computer system, services and network. All access and activity that is logged can be tracked back to your username

6. Viruses and Malicious Code

Viruses, spyware, hacking tools are categorised as malicious code and are a risk to The Romero Catholic Academy Network System. Web sites that are identified causes of computer viruses and malware are blocked. Users should use suitable caution when accessing Web sites.

Do

- ✓ Take all necessary precautions when downloading files from the internet or attached to emails.
- ✓ Take steps to secure your computer when leaving it for a few minutes to avoid the risk of interfering or misuse, or breach of GDPR e.g. by locking the screen.
- ✓ Delete spam, chain, and other junk email without forwarding.
- ✓ Inform IT Services immediately if you think that your computer may have a virus.
- ✓ Ensure that any equipment not belonging to the school you use to access Academy systems are free from malicious code e.g. check with an up to date anti-virus software

Do Not

- ✗ Deliberately, or carelessly allow malicious code or any other unwanted program or file onto any Academy systems.
- ✗ Port, security scan the network.
- ✗ Bypass user authentication or security of any system, network or account.
- ✗ Use any program, script, command, or send messages of any kind with the intent to interfere with, or disable via any means, locally or via the Internet.
- ✗ Use removable storage e.g., CD, DVD, USB
- ✗ Introduce malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- ✗ Deliberately circumvent any precautions taken to prevent malicious code accessing School systems e.g. by disabling antivirus software
- ✗ Open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then empty your deleted items

7. Use of Academy Email – Applicable to Primary, Secondary and Shared Services Team

The Romero Catholic Academy staff will correspond with email using **romeromac.com** email address, when communicating externally and internally.

The Academy provides E-mail to pupils to enable them to communicate effectively and efficiently with other members of staff and pupils. The Academy uses Microsoft 365 for Education. By logging into the Microsoft account, you are not to use the account to send spam, distribute viruses or otherwise abuse the service. All users are subject to these agreements, which conform to the Microsoft Acceptance Terms.

When using The Romero Catholic Academy E-mail facilities, you should comply with the following:

Do

- ✓ Check your E-mail regularly to see if you have any messages.
- ✓ Include a meaningful subject line in your message.
- ✓ Check the address line before sending a message and check you are sending it to the right person
- ✓ Delete E-mail messages when they are no longer required.
- ✓ Respect the legal protections to data and software provided by Microsoft for Education copyright and licenses
- ✓ Take care not to express views, which could be regarded as offensive or defamatory.

Do Not

- ✗ Expect an immediate reply, the recipient might not be at their computer or could be too busy to reply straight away. We do have an email protocol to refrain from emailing after 7pm on a Friday until 4pm on Sunday to aid wellbeing.
- ✗ Forward E-mail messages sent to you personally to others, particularly newsgroups or mailing lists, without the permission of the originator.
- ✗ Use E-mail for personal reasons.
- ✗ Send excessively large E-mail messages or attachments.
- ✗ Send unnecessary messages such as celebratory greetings or other non-work items by E-mail, particularly to several people.
- ✗ Participate in chain or pyramid messages or similar schemes.
- ✗ Represent yourself as another person.
- ✗ Use electronic mail to send or forward material that could be construed as confidential, political, obscene, threatening, offensive or defamatory.

8. Use of Academy internet

The Romero Catholic Academy provides Internet access to pupils to assist them in their education. It is expected that it will be used to research information concerning their courses and coursework material. It should not be used for personal reasons. You may only access the Internet by using The Romero Catholic Academy’s Web content scanning software, firewall and router.

Do

- ✓ Keep your use of the Internet to a minimum.
- ✓ Check that any information you access on the Internet is accurate, complete and current.
- ✓ Check for validity of information.
- ✓ Respect the legal protections to data and software provided by copyright and licenses.
- ✓ Inform the IT Team immediately of any unusual incidence.
- ✓ Inform the IT Team immediately if you mistakenly access material that is profane or obscene.

Do Not

- ✗ Download content from Internet sites except if it is course work related.
- ✗ Download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
- ✗ Download software from the Internet and install it on the School’s computer system.
- ✗ Use the Academy's computers to make unauthorised entry into any other computer or network.
- ✗ Disrupt or interfere with other computers or network users, services, or equipment.
- ✗ Intentional disruption of the operation of computer systems and networks
- ✗ Represent yourself as another person.
- ✗ Use Internet access to transmit confidential, political, obscene, threatening, or harassing materials
- ✗ Arrange, over the internet, to meet strangers, or give out any of your personal information.
- ✗ Access unauthorised chat rooms.

9. Use of Social Media

Facebook, Twitter, email and other online social networks play a key part in the lives of pupils. Given the rapid increase of social media, it is impossible to list all possible types of media as they are constantly increasing. The Romero Catholic Academy pupils are not permitted to access social media websites from the Academy's computers or other academy devices at any time, except authorised by the Principal or relevant member of the Leadership team.

The Academy appreciates that pupils may use social media in a personal capacity. However, pupils must be aware that if they are known from their user profile as being related with the school, views they express could be considered to reflect the academy's opinions and so can damage the name of the school.

For this reason, they should avoid mentioning the academy by name, or any member of staff by name or position or any details relating to the academy. Opinions offered should not bring the academy into disrepute, breach confidentiality or copyright, or bully, harass or discriminate in any way.

Communications to all pupils and to all online communications which directly or indirectly, represent the school, and to such online communications posted at any time and from anywhere. If an academy user carelessly takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Do

- ✓ Consider the copyright of the content you are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- ✓ Ensure that use of social media does not infringe upon relevant data protection laws, or breach confidentiality.
- ✓ Report to the IT Team if inappropriate content is accessed online on school premises.
- ✓ Verify links, attachments, downloads, emails or any other received items.

Do Not

- ✗ Access social media in school at in appropriate times
- ✗ Create or transmit material that might be defamatory or incur liability for the Romero Catholic Academy.
- ✗ Post message, status updates or links to material or contact that is inappropriate.
- ✗ Upload pictures online other than via school owned social media accounts.
- ✗ Disclose any confidential information to third parties.
- ✗ Link to your own blog or other personal web pages to the school website.
- ✗ Make comments, post content or link to materials that will bring the school into disrepute.
- ✗ Give away your password or use the same password for any other services.
- ✗ Post content that could easily be viewed as obscene, threatening or intimidating or even might constitute harassment or bullying.
- ✗ Publish confidential or commercially sensitive material.
- ✗ Breach copyright, data protection or other relevant legislation.
- ✗ Attempt to bypass the network's firewalls to access social media.
- ✗ Give out personal information, or post personal images to people you talk to online.
- ✗ Arrange to meet somebody you have only met online.
- ✗ Believe everything you read, very sources and content of information.

10. When Pupils/ Pupils Leave School

Pupil school profiles will be suspended and subsequently deleted when pupils either move to another educational establishments or terminate their studies at The Romero Catholic Academy.

Pupils/ Students must make all efforts to transfer important files from the School file space before they finish their journey of learning at a school within The Romero Catholic Academy. No responsibility will be taken by the School for the loss of data deleted in respect to the termination of study and deletion of pupil/ student accounts.

If you discover a security problem, for example being able to access other user's data, you must inform IT Services immediately and not show it to other users. Pupils known as a security risk will be denied access to the network

11. Monitoring

The Romero Catholic Academy maintains the right to examine any systems and inspect any data recorded in those systems. In order to ensure compliance with this policy, the school will use monitoring software in order to check upon the use and content of emails periodically. Such monitoring is for legitimate purposes only.

If the School suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the academy will terminate or restrict usage. If the academy suspects that the system may be being used for criminal purposes then the matter may be brought to the attention of the relevant law enforcement organisation.

12. Non Compliance

Use and access to resources within The Romero Catholic Academy and information is conditional upon adherence to the Acceptable Use Policy. Where there is found to have been a deliberate attempt at unauthorised access, or wilful carelessness to protect the academy information systems and data, the academy will initiate the appropriate disciplinary processes.

It is your responsibility to report suspected breaches of security policy without delay to the IT Team. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with The Romero Catholic Academy Behaviour (Pupils/ Staff) or Disciplinary (Staff) Policy.

Disciplinary can vary depending upon the severity of the offence, from a recorded verbal warning, written warning, temporary withdrawal of internet use, suspension of all account activity to school exclusion. Any breach of any law may lead to criminal proceeding.

13. Exemptions

Any exception to the policy must be approved by Catholic Senior Executive Leader or the Principal or the Head of IT.

14. Links to other policies

This Acceptable Use Policy is linked to our;

- Behaviour Policy
- Disciplinary Policy
- E Safety Policy
- No Platform Policy
- Social Media Policy
- Stress and Wellbeing Policy
- Whistleblowing Policy

15. Monitoring and Review

The Board of Directors delegate the implementation of this policy to the Governing Body. This policy will be reviewed by CC3 Quality, Provision, Performance and Standards.

16. External Documents

All users must conform to all applicable regulation and legal precedent, including the requirements of the following specifically related Acts of Parliament, or any reform thereof:

- Malicious Communications Act 1988
- Computer Misuse Act 1990
- Data Protection Act 1998
- The copyright, designs and patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Communications Act 2003
- Counter-Terrorism and Security Act (2015)
- SANS
- Microsoft Privacy Statement

Appendix 1

Pupil Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Pupils should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the academy will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating online.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people offline that I have communicated with online, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the Academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g., YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the academy:

- I will only use my own personal devices (mobile phones) in school if I have permission.
- I understand that, if I do use my own devices in the academy, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering /security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Appendix 2

Pupil Acceptable Use Policy Agreement

Primary School

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (parent/ carer): ....

Appendix 3

Pupil Acceptable Use Agreement

Secondary School

This form relates to the Pupil Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use The Romero Catholic Academy systems and devices (both in and out of school where applicable)
- I use my own devices in the academy (not allowed on school network systems) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the academy in a way that is related to me being a member of this academy eg communicating with other members of the school, accessing school email, website etc.

Name of Pupil: --

Group / Class: --

Signed: --

Date: --

Parent/Carer Countersignature applicable to pupils under the age of 13 years old

Please ensure we have a completed and signed a photograph consent form for you along with your consent for use of Biometric data (fingerprint for school meal purposes only)

Appendix 4

Parent/Carer Acceptable Use Agreement

Primary School

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Pupils should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that pupils will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents/ Carers are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name: ....

Student / Pupil Name:__ ....

As the parent/carer of the above pupil, I give permission for my son/daughter to have access to the internet and to IT systems at school.

I understand that the school has discussed the Acceptable Use Agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Please also ensure we have a completed and signed a photograph consent form for your son/daughter

Appendix 5

Parent/Carer Acceptable Use Agreement

Secondary School

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name: ....

Student / Pupil Name:__ ....

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Please also ensure we have a completed and signed a photograph consent form for your son/daughter along with consent for Biometric data (fingerprint for school meal purposes only)

Appendix 6

Staff (and Volunteer) Acceptable Use Agreement

New technologies have become integral to the lives of everyone in today's society, both within academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *academy* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, cloud based apps etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using academy IT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with The Romero Catholic Academy Data Protection policy/Information Security Policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website/CLOUD BASED APPS) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school / academy:

- When I use my mobile devices (laptops/tablets/mobile phones etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the academy IT systems unless permission is sought for exceptions (e.g. Ofsted communication)
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant academy policies.
- I **will not** upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in academy policies.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the The Romero Catholic Academy Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of academy digital technology equipment in school, but also applies to my use of academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Local Governing Body, Directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

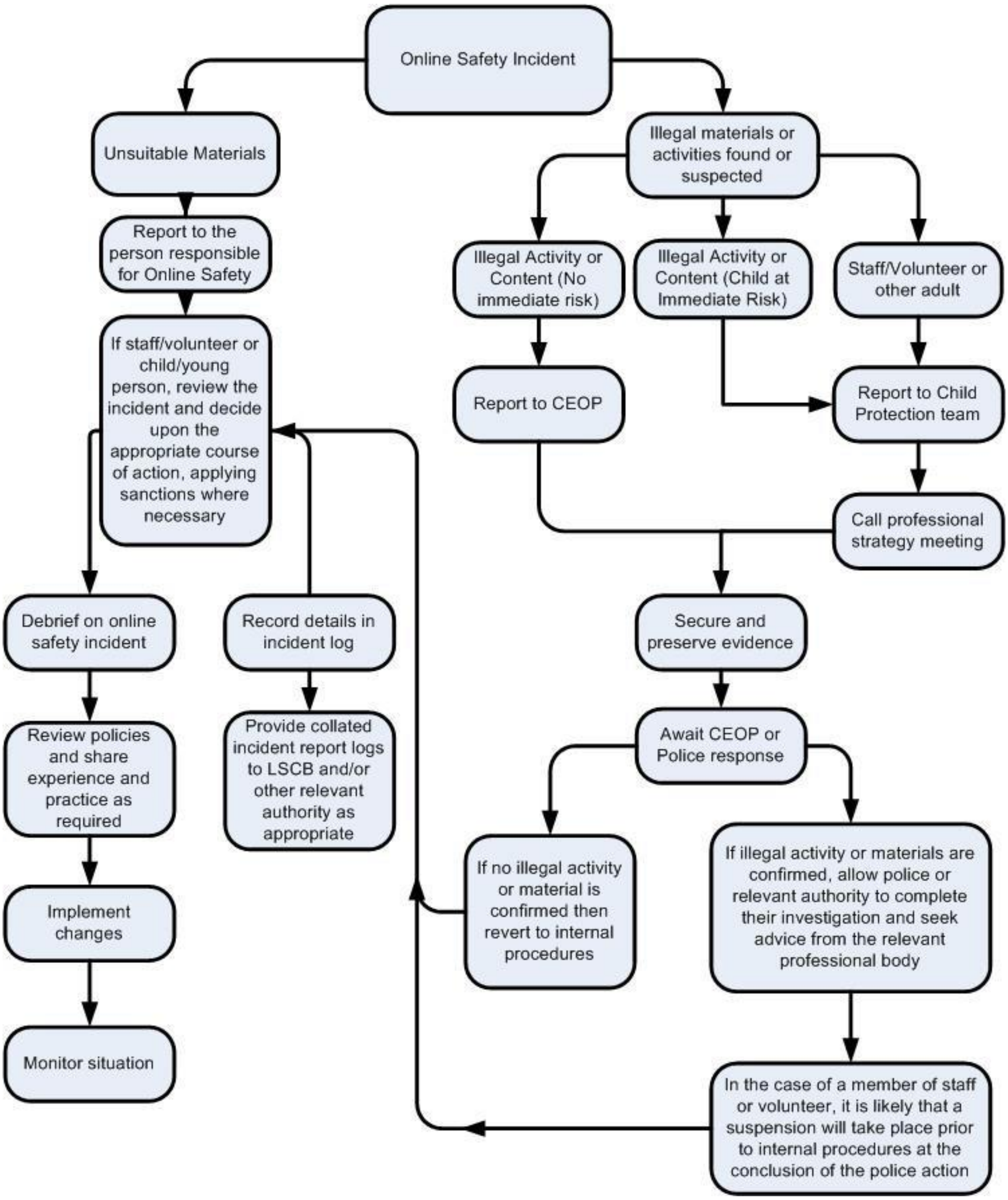
Staff / Volunteer Name:...

Signed: ....

Date: ....

Appendix 7

Responding to incidents of misuse – flow chart


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action