Artificial Intelligence and E-Safety (AI) Policy

Responsible for policy: **CC3: Quality Provision and Performance**
Review: **Triennial**
Chair of Directors

Contents

1. Definitions

In this **E Safety & AI 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 **E Safety & AI 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**, **SS Peter and Paul**, **St Gregory**, **St John Fisher**, **St Patrick**, **Cardinal Wiseman**, **Shared Services Team**.

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 Clerk to the Board or the Clerk to the Local Academy Committee of the Academy appointed from time to time, as appropriate.

v '**Chair'** means the Chair of the Board of the Directors or the Local Academy Committee appointed from time to time.

vi '**Chief Education Officer (CEO)** 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 **Principal'** means the substantive Principal, who is the person with overall responsibility for the day to day management of the school.

x '**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.

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

xii '**Vice-Chair'** means the Vice-Chair of the Academy Committee elected from time to time.

xiii **'Head of IT'** means the person responsible for IT/Computing across the Academy

xiv **'IT Team'** means the team of staff supporting the Head of IT and the individual academies

xv **'Artificial Intelligence' (AI)** means the simulation of human intelligence by machines, including systems capable of learning, reasoning, problem-solving, and decision-making.

xvi **'AI Tools'** means software or platforms that incorporate AI functionality.

xvii '**Pupils** means Pupils (EYFS), Pupils (KS1-KS4), Students (KS5). For the purposes of the policy we will use pupil throughout.

2. Development, Monitoring and Review of this Policy

This E-Safety & AI policy has been updated by members from: Board, CEO, Principals, Head of IT, School Improvement.

3. Schedule for Review of this Policy

This policy was approved by Core Committee	CC3
The implementation of this policy will be monitored by the:	Core Committee 3 Quality Provision and Performance
Monitoring will take place at regular intervals:	Annually
The Board of Directors/Core Committee will receive a report on the implementation of the policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually through the Principal reports
The policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	
Should serious online safety incidents take place, the following external persons/agencies should be informed:	***Please see Appendix 1 for list of contacts***

The school will monitor the impact of the policy using:

- Firewall, Lightspeed
- Internal monitoring of website activity. All alerts are directed to Designated Safeguarding Leads (DSL) in each school across the MAC
- Logs of reported incidents (DSL will complete logs)
- Monitoring logs of internet activity (including sites visited)/filtering

4. Scope of the Policy

This policy applies to all members of The Romero Catholic Academy (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of the Academy digital technology systems, both in and out of The Romero Catholic Academy.

The Education and Inspections Act 2006 empower principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off The Romero Catholic Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of The Romero Catholic Academy but is linked to membership of the academy. The 2011 Education Act increased these powers about the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Relationship and Positive Behaviour Policy.

The Romero Catholic Academy will deal with such incidents within this policy and associated behaviour and anti- bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

5. Roles and Responsibilities

Board of Directors

Core Committee 3 are responsible for the approval of the E-Safety & AI Policy and for reviewing the effectiveness of the policy. This will be carried out by the Board receiving regular information about online safety incidents and the effective use of AI technologies.

Principal and Senior Leaders

- The Principal of each school has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the DSL/E Safety Coordinator
- The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority/MAC/other *relevant body* disciplinary procedures). Online Safety BOOST includes an 'Incident Response Tool' that outlines the steps (and forms to complete) any staff facing an issue, disclosure or report, need to follow. More information is available at: https://boost.swgfl.org.uk/ Please see our Whistleblowing Policy
- The Principal is responsible for ensuring that the E Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. The Academy needs to ensure that Induction Training for E Safety is built into Safeguarding Training. This training can be a presentation or online training. It can be delivered by computing Subject Lead/E Safety in each school. A document to be signed as per safeguarding training. This links in with Acceptable Use Policy
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Principal will receive regular monitoring reports from the monitoring tool in place
- The Principal will encourage the effective use of AI to support and enhance the MAC's goals, not to replace human judgement.

Head of IT

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies
- ensures that the technical infrastructure is in place, maintained and updated to support e-safety (e.g. firewall, backup, Internet monitoring, filtering systems)
- Advises E-Safety Coordinator and Principal on technical trends and issues concerning the IT infrastructure and online access
- Liaises with school IT technicians
- CEO will be given access to portal for monitoring logs across The Romero Catholic Academy
- Ensures that accessible AI tools comply with data protection laws and protect the privacy of individuals
- Provide resources and guidelines to ensure staff are competent in the use of AI technologies

IT Team

The IT Team is responsible for ensuring:

- that The Romero Catholic Academy technical infrastructure is secure and is not open to misuse or malicious attack
- that The Romero Catholic Academy meets required online safety technical requirements and any Online Safety Policy that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy should be applied and updated on a regular basis and that its implementation is not the sole

responsibility of any single person (see appendix "Technical Security Policy Template" for good practice)
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the CEO, Principal and Head of IT for investigation
- that monitoring software/systems are implemented and updated as agreed in academy policies

Pupils
- are responsible for using The Romero Catholic Academy's digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that The Romero Catholic Academy E Safety Policy covers their actions out of school, if related to their membership of the school **(Applicable to Cardinal Wiseman Secondary School)**
- should be provided with regular E Safety lessons of 'How to stay safe online' – Education for a Connected World using the https://projectevolve.co.uk/
- should report any computing misuse or viewing of inappropriate content to a teacher
- should seek help from an adult if they face problems

Parent/Carers
Parents/Carers play a crucial role in ensuring that their pupils understand the need to use the internet/mobile devices in an appropriate way. The Romero Catholic Academy will take every opportunity to help parents
understand these issues through parents' evenings, newsletters, letters, website, information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support The Romero Catholic Academy in promoting good online safety practice and to follow guidelines on the appropriate use of:
- digital and video images taken at school events
- access to parents' sections of the parent contact portal
- their children's personal device and storage in the academy including mobile phones, iPads and laptops

Staff
- Implement the E Safety & AI Policy
- Must have read, understood and signed the Staff Acceptable Use Policy
- Must report any suspected misuse or problem to the E Safety Coordinator for investigation
- Ensure pupils understand and follow the E Safety Policy and Acceptable Use agreement
- Ensure E-Safety issues are embedded in all aspects of the curriculum and other activities – this should be
  updated regularly to include relevant issues such as grooming and sexting
- Maintain professional conduct when online, both inside and outside of the academy
- Maintain accountability for decisions made using AI tools and not delegate full authority
- Ensure materials obtained from AI tools do not infringe copyright law.
- Ensure only approved AI tools are used for processing sensitive or confidential organisational data

Acceptable Use Policies
The Romero Catholic Academy ensure all staff and pupils adhere to the Acceptable Use Policy. The policy will cover the requirement for the user to use the computing equipment for legitimate purposes, act within a remit appropriate to their professional/pupil status, employ e-safety practices consistently and follow procedures regarding e-safety. Staff and Pupils are required to sign an Acceptable Use Agreement before being granted to use the academy's portable devices. ***Please see Acceptable Use Policy for template forms.***

6. Policy Statements

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the Academy's online safety provision. Pupils and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision- making.
- Pupils should be helped to understand the need for the pupil Acceptable Use Policy/Agreement and encouraged to adopt safe and responsible use both within and outside academy.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, staff may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Team can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. DSL to include this on Monitoring Log.

Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their pupils and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often pupils and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The Romero Catholic Academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, websites and social media
- Parents/Carers evenings
- High profile events/campaigns e.g. Safer Internet Day

Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy AI E Safety Policy and Acceptable Use Policy.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Head of IT will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The Principal/E Safety Coordinator will provide advice/guidance/training to individuals as required.

Directors/Local Governing Body

Directors and LGB should take part in online safety training/awareness sessions, with particular importance for those who are members of any committee/group involved in technology/online safety/health and safety/safeguarding. Training provided as per staff training.

7. Infrastructure, Equipment, Filtering and Monitoring

The Romero Catholic Academy IT Network Team will be responsible for ensuring that academy network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- The Romero Catholic Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of the academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to the academy technical systems and devices.
- All users **will be provided with a username and secure password by** each school within The Romero Catholic Academy who will keep an up-to-date record of users and their usernames. **Users are responsible for the security of their username and password** and will be required to change their password regularly
- The "administrator" passwords for the academy computing systems, used by the Head of IT and/or IT Team will not be shared according to GDPR regulations
- Head of IT is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored.
- Internet filtering/monitoring should ensure that pupils are safe from terrorist and extremist material when accessing the internet.
- The Romero Catholic Academy has provided enhanced/differentiated user-level filtering
- The Romero Catholic Academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy
- An appropriate system is in place with GDPRis for School Business Managers/Office Managers to report any actual/potential technical incident/security breach to the relevant person, as agreed). GDPR Breaches must be reported to DPO in each school and then passed on to the MAC DPO.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The academy network infrastructure and individual workstations are protected by up-to-date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" Trainee Teachers and Supply Teachers use academy owned teaching devices
- An agreed policy is in place regarding the extent of personal use that users (staff/pupils) are allowed on school devices that may be used out of school with school logins
- The Romero Catholic Academy's Information Security Policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- The Romero Catholic Academy's Information Security Policy *is in place regarding the use of removable media and data encryption(eg memory sticks) by users on school devices.* ***Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured****.*

8. Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

The school Acceptable Use Policy for staff, pupils and parents/carers will consider the use of mobile technologies:

Primary School	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Left in school office*	*Yes* ***device must be locked away and not for work use***	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
No network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*Guest Wi-Fi*

Secondary School	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes* ***device must be locked away and not for work use***	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
No network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*Guest Wi-Fi*

9. Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the

taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website/social media/local press. Acceptable Use Agreements as well as Photograph Consent Forms should be completed at the start of each Academic Year
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their pupils at academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment, the personal equipment of staff should not be used for such purposes and stored to a school monitored and audited storage systems (The Academy Network or G-Suite/Office 365)
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers dependent on age of pupil

10. Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The Romero Catholic Academy must ensure that:

- It has a Data Protection, Information Security and a Freedom of Information Policy which sets out how it will deal with FOI requests.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO)
- It has appointed a Data Protection Officer (DPO)
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in The Romero Catholic Academy Privacy Notices.
- Data Protection Impact Assessments (DPIA) are carried out.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- All staff receive data protection training and are made aware of their responsibilities.

The Romero Catholic Academy Information Security Policy will ensure Staff:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

11. Communication

When using communication technologies, the academy considers the following as good practice:

- The Romero Catholic Academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the academy email service to communicate with others when in school, or on academy systems.
- Users must immediately report to the nominated person – in accordance with policy the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff, pupils or parents/carers (email, social media, chat etc) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on The Romero Catholic Academy website and only official email addresses should be used to identify members of staff.

12. Social Media – Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy liable to the injured party. Reasonable steps to preventable harm must be in place.

The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues. Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or academy staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to The Romero Catholic Academy
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When The Romero Catholic Academy social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under academy disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy

- Personal communications which do not refer to or impact upon the academy are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The Romero Catholic Academy permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

13. Dealing with inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in an academy context, either because of the age of the users or the nature of those activities.

The academy believes that the activities referred to in the following section would be inappropriate in a school / academy context and that users, as defined below, should not engage in these activities in / or outside the school / academy when using school / academy equipment or systems. The school / academy policy usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Pupils Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against pupils Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy					X	
Infringing copyright					X	

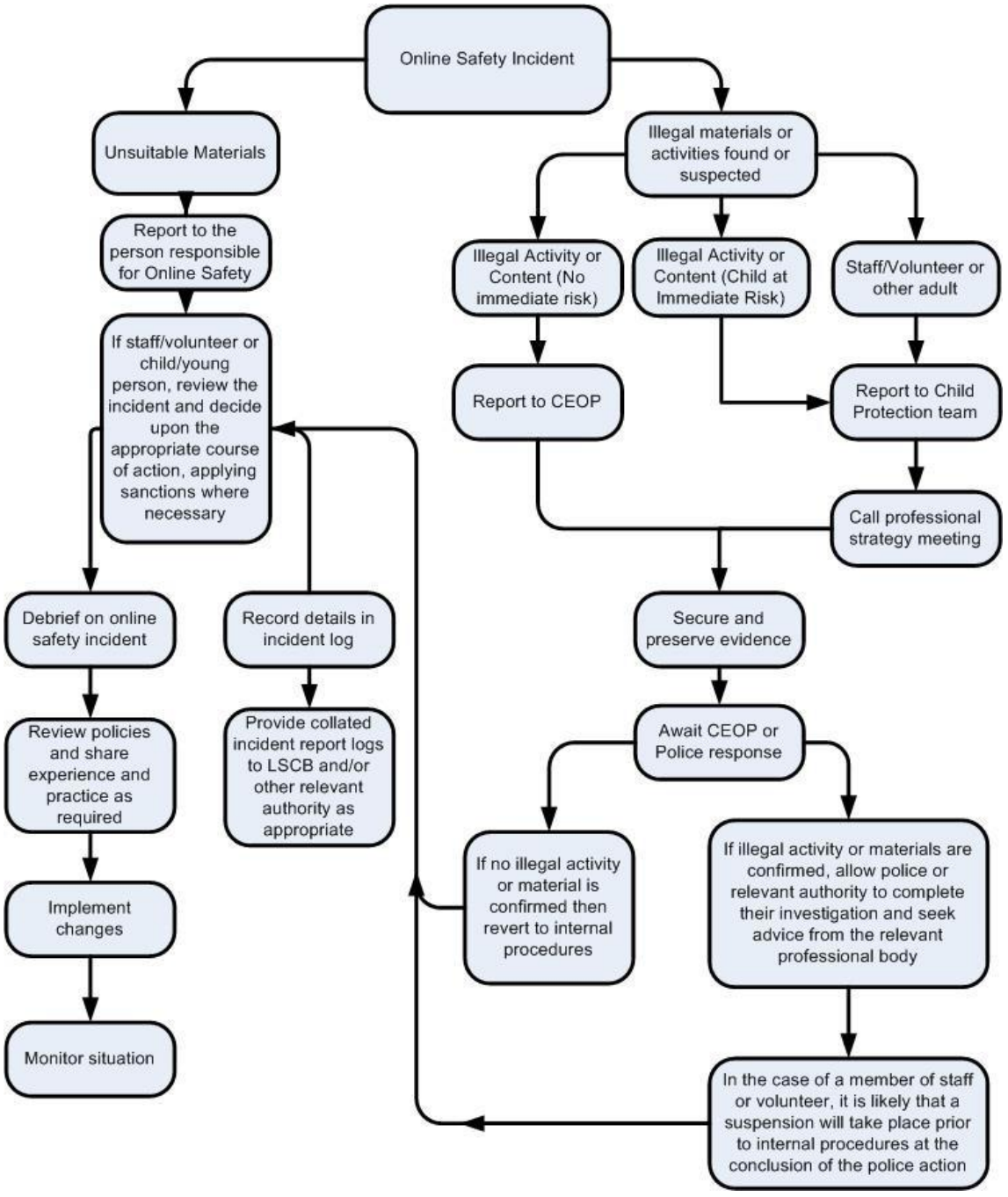
Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading /uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X	X		
On-line gaming (non-educational)				x	
On-line gambling				x	
On-line shopping/commerce				x	
File sharing					
Use of school social media			x		
Use of messaging apps				x	
Use of video broadcasting e.g. Youtube			x		

14. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the flowchart below for responding to online safety incidents and report immediately to the police.



Other incidents

It is hoped that all members of The Romero Catholic Academy will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action
    -

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials
-

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation

It is important that all of the above steps are taken as they will provide an evidence trail for the academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

15. The Romero Catholic Academy's Actions and Sanctions

It is more likely that academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Any of the following:	**Actions/Sanctions**								
Pupils Incidents	**Refer to class teacher**	**Refer to Head of Department/Year**	**Refer to CEO/Principal**	**Refer to Police**	**Refer to technical support for action re filtering/security**	**Inform parents/carers**	**Removal of network/internet access rights**	**Warning**	**Further sanction eg detention/exclusion**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section).			X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X	X						X	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X				X		X	
Unauthorised/inappropriate use of social media/messaging apps/personal email	X	X				X		X	
Unauthorised downloading or uploading of files	X	X			X			X	
Allowing others to access academy network by sharing username and passwords	X	X				X	X		X
Attempting to access or accessing the academy network, using another pupil's account	X	X				X	X		X
Attempting to access or accessing the academy network, using the account of a member of staff	X	X				X	X		X
Corrupting or destroying the data of other users	X	X				X	X	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X		X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X				X		X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the school		X	X			X			X
Using proxy sites means to subvert the academy's filtering system		X			X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X				X	X		X	
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X		X	X	X		X

Any of the following:	Actions/Sanctions							
Staff Incidents	Refer to Line Manager	Refer to CEO/Principal	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section)	X	X	X	X	X			X
Inappropriate personal use of the internet/social media/personal email	X					X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X			X	X		
Deliberate actions to breach data protection or network security rules	X	X	X		X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X		X	X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X		
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils	X	X	X		X			X
Actions which could compromise the staff member's professional standing	X						X	
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy		X	X			X		
Using proxy sites or other means to subvert the academy's filtering system	X	X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
Breaching copyright or licensing regulations	X	X			X	X		
Continued infringements of the above, following previous warnings or sanctions		X	X					X

16. Links to other policies

This E Safety and AI Policy is linked to our;

- Acceptable Use Policy
- Data Protection Policy (including Subject Access Requests)
- Information Security Policy
- Freedom of Information Policy
- Disciplinary Policy
- Relationship and Positive Behaviour Policy
- Whistleblowing Policy

Appendix 1 – Useful Contacts

Service	Tel	Email	Website
Coventry Safeguarding Pupils Partnership	02476 975477	CoventryCSCP@coventry.gov.uk	Coventry CSCP
LADO	02476 975483	lado@coventry.gov.uk	LADO