St Margaret Ward Catholic Academy

E-Safety Policy

Let us remember we are in the presence of God »

Policy Adopted	Next Review	Author
JANUARY 2020	JANUARY 2021	MR P JOHNSON

Agreed by Governors	Date
Mr D Bailey - Chair	JANUARY 2020

E-Safety Data Security and
Guidance Policies for ICT
Acceptable Use

Introduction:

Roles and Responsibilities:

- Governors
- Principal and Senior Leaders
- E-Safety Coordinator / Officer
- Network Manager / Technical Staff
- Teaching and Support Staff
- Child Protection / Safeguarding Designated Person / Officer
- E-Safety Committee
- Students / Pupils
- Parents / Carers
- Community Users

Policy Statements:

- Education - Students / Pupils
- Education - Parents / Carers
- Education- The Wider Community
- Education and training - Staff / Volunteers
- Training - Governors
- Technical- infrastructure / equipment, filteri.ng and monitoring
- Bring your own devices (BYOD)
- Use of digital and video images
- Data protection
- Communications
- Social Media- Protecting Professional Identity
- User Actions- unsuitable / inappropriate activities
- Responding to incidents of misuse

Appendices:

- Student / Pupil Acceptable Use Policy Agreement Template- older children
- Parents / Carers Acceptable Use Policy Agreement Template
- Staff and Volunteers Acceptable Use Policy Agreement Template
- Responding to incidents of misuse- flowchart
- School Reporting Log template
- School Training Needs Audit template
- School Technical Security Policy template (includes password- security and filtering)
- School Personal Data Policy template
- School Policy Template- Electronic Devices- Search and Deletion
- School Bring Your Own Devices (BYOD) Template Policy
- School E-Safety Group Terms of Reference
- Glossary of Terms

Development / Monitoring / Review of this Policy:

This E-safety policy has been developed by a working group / committee made up of:

- Vice Principal – P Johnson
- Staff- including Teachers, Support Staff, Technical staff
- Safeguarding Manager– A Holdcroft
- Parents and Carers
- Students

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

- This e-safety policy was approved by the Academy Committee January 2021
- The implementation of this e-safety policy will be monitored by P Johnson
- Monitoring will take place at regular intervals: led by P Johnson during the Summer Term 2021
- The Academy Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e- safety incidents) at regular intervals.
- The E-Safety 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 e-safety or incidents that have taken place. The next anticipated review date will be: July 2021
- Should serious e-safety incidents take place, the following external persons / agencies should be informed: LADO and also WM Police

The school will monitor the impact of the policy:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of: students, pupils, parents, carers and staff

Scope of the Policy:

This policy applies to all members of the St Margaret Ward Catholic Academy community (including staff, students *I* pupils, volunteers, parents, carers, visitors, community users) who have access to and are users of St Margaret Ward Catholic Academy ICT systems, both in and out of the St Margaret Ward Catholic Academy.

The **Education and Inspections Act 2006** empowers the Principal to such extent as is reasonable, to regulate the behaviour of students *I* pupils when they are off the *St Margaret Ward Catholic Academy* site and empowers members of staff to impose disciplinary penal ties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the St Margaret Ward Catholic Academy but is linked to membership of the St Margaret Ward Catholic Academy.

The **2011 Education Act** increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published SMWCA Behaviour Policy.

The St Margaret Ward Catholic Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents *I* carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities:

The following section outlines the e-safety roles and responsibilities of individuals and groups within the St Margaret Ward Catholic Academy*:*

Governors *I* Academy Committee:

Directors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Academy Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Academy Committee has taken on the role of E-Safety Director. The role of the E-Safety Director will include:

- Regular meetings with the E-Safety coordinator Officer
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering change control logs
- Reporting to relevant Academy Committee Meetings

Principal and Senior Leaders:

- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e- Safety will be delegated to the E-Safety Co-ordinator Officer. Sufficient time will be allowed for these duties to be carried out.

- The Principal and Assistant Principal and with members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

- The Principal/ Senior Leaders are responsible for ensuring that the E-Safety Coordinator Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues as relevant.

- The Principal/ Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. Day to day responsibility for this is with Academy Network Manager Mr D Millward.

- The Senior Leadership Team and Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator Officer.

The E-Safety Officer will:

- Lead the e-safety committee
- Take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies *I* documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff inset September 2021.
- Liaises with the Local Authority *I* relevant body
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with E-Safety Governor/ Director to discuss current issues, review incident logs and filtering *I* change control logs
- Attends relevant meeting *I* committee of Governors/ Directors
- Report regularly to Senior Leadership Team

Sanctions will be issued and dealt with in line with the schools Behaviour Policy, by the relevant member s of staff.

Network Manager *I* Technical staff:

- St Margaret Ward Catholic Academy has a self-managed ICT service controlled by the network manager Mr D Millward, it is the responsibility of the St Margaret Ward Catholic Academy to ensure that all the e-safety measures that are the responsibility of the school technical staff, as suggested below;
- The Network Manager Technical Staff Co-ordinator for ICT Computing is responsible for ensuring:
- That the St Margaret Ward Catholic Academy's technical infrastructure is secure and is not open to misuse or malicious attack
- That the St Margaret Ward Catholic Academy E-safety meets required e-safety technical requirements and any Local Authority or other relevant body E-Safety Policy Guidance 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 is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network, internet, and remote access email is regularly monitored in order that any misuse I attempted misuse can be reported to the Principal/ Senior Leader; E-Safety Coordinator Officer for investigation, action or sanction.
- That monitoring software systems are implemented and updated as agreed in St Margaret Ward Catholic Academy policies.

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current St Margaret Ward Catholic Academy e-safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy Agreement (AUP).
- They report any suspected misuse or problem to the Safe guarding team as identified in the staff handbook for investigation / action / sanction.
- All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Students understand and follow the e-safety and acceptable use policies.
- Student's pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned students/ 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.

Child Protection / Safeguarding Designated Officer:

Should be trained in e-safety issues and be aware of the potential for serious child protection Safe guarding issues to arise from:

- Sharing of personal data.
- Access to illegal / inappropriate materials.
- Inappropriate on-line contact with adults I strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

E-Safety Group:

The E-Safety Group provides a consultative group that has wide representation from the St Margaret Ward Catholic Academy community, with responsibility for issues regarding e-safety and the monitoring the E-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body and Directors.

Members of the E-safety Group will assist the e-Safety Coordinator Officer with:

- The production, review, monitoring of the school e-safety policy documents.
- The production, review, monitoring of the school filtering policy and requests for filtering changes.
- Mapping and reviewing the e-safety curricular provision - ensuring relevance, breadth and progression.
- Monitoring network, internet and incident logs.
- Consulting stakeholders- including parents/carers and the students I pupils about the e-safety provision.
- Monitoring improvement actions identified through use of the 360-degree safe self review tool.

An E-Safety Group Terms of Reference Template can be found in the appendices.

Students:

The 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At St Margaret Ward Catholic Academy, we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviour and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-today activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PC's, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

Personal Use:

Personal use of ICT resources by School staff is permitted, subject to the following conditions:

- Personal use of the internet does not conflict with normal operational requirements;
- That the facilities are not used for the promotion of a political party, a candidate or group of candidates in an election or in connection with a party-political campaign;
- That the facilities are not used for private business purposes or financial gain;

- The St Margaret Ward Catholic Academy cannot be held responsible or liable for any personal loss suffered as a result of personal use of ICT resources.

Permitted personal use of ICT resources **does not extend to**:

- Using personal internet e-mail accounts (e.g. hotmail, lycos, yahoo) - unless these have been authorised by the Principal and the school web filtering policy is set accordingly.
- The words "Personal E-mail" should be included in the subject field of any e-mail intended to be personal.

Education- students *I* pupils:

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

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

- A planned e-safety curriculum should be provided as part of the ICT Programme and other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial *I* pastoral activities
- Students 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.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the Student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- 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 students 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 students 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, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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.

Education – Parents/Carers:

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

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site,
- Parents /Carers evenings sessions

Also:

- High profile events, campaigns e.g. Safer Internet Day
- Reference to the relevant web sites and publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training Staff and Volunteers:

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the E-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme; ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator Officer will receive regular updates through attendance at external training events (e.g. from SGFL, LA or other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff team meetings and Inset days.
- The E-Safety Coordinator Officer will provide advice guidance training to individuals as required.

Training- Governors/Directors:

Governors / Directors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies/ lessons).

Monitoring:

It is the St Margaret Ward Catholic Academy's responsibility to ensure that the ICT service, has carried out all the e-safety measures, as suggested below.

The Academy will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- St Margaret Ward Catholic Academy technical systems will be managed in ways that ensure that the St Margaret Ward Catholic Academy meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school
- technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to St Margaret Ward Catholic Academy technical systems and devices.
- All users will be provided with a username and secure password by L Bloor (school office manager) and Mr D Millward (Network Manager) 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 every year.
- The administrator passwords for St Margaret Ward Catholic Academy ICT system, used by the Network Manager must also be available to the Principal or other nominated senior leader and kept in a secure place (e.g. school safe)
- E Stanway (Business Manager) is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content 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. There is a clear process in place to deal with requests for filtering changes.
- The school has provided enhanced I differentiated user-level filtering.
- The academy also use Smoothwall filtering and Impero for use in classrooms.

St Margaret Ward 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 Agreement.

- An appropriate system is in place, in first instance reporting to members of the ICT teaching team and the Safeguarding Team, for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work-stations, mobile devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested

regularly. The school 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" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. On the first visit to St Margaret Ward Catholic Academy, visitors wishing to access the schools system will be asked to sign an AUA and these will be held by L Bloor office manager.
- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks, CDs and DVDs) 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.

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

- ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

- ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

- All monitoring, surveillance or investigative activities are conducted by ICT- authorised staff and comply with the Data Protection Act 1998,the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

- Personal digital devices used on school premises may be included in this monitoring if used in conjunction with an educational activity (recording images for a project etc.)

- Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

AND

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised St Margaret Ward Catholic Academy staff.

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the LA Disciplinary Procedure.

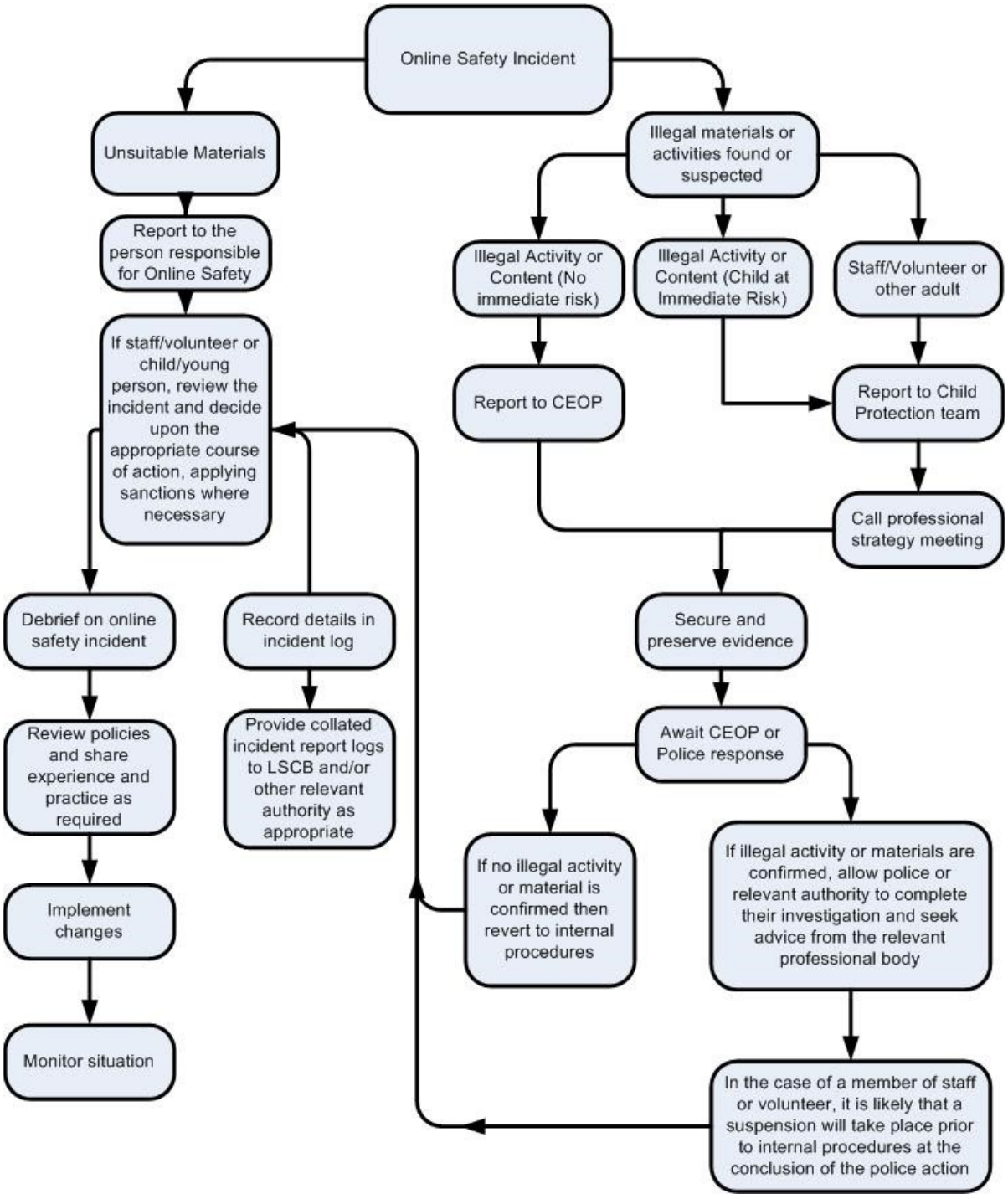
Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting:

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's e Safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorized use of ICT and all other policy non-compliance must be reported to your network manager or safety coordinator

Please refer to the relevant section on incident reporting, E \-Safety Incident Log & Infringements.

Responding to incidents of misuse- flow chart



St Margaret Ward Catholic Academy Policy

- 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. Young people should have an entitlement to safe internet access at all times. This policy will be annually reviewed and will be brought to the attention of parents through school website, parent information evening and in planners. New entrants to the school also receive a letter about access to the school network and use of social media in welcome packs.

Acceptable Use Agreement: Pupils

This Acceptable Use Policy 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 users at risk.
- The school will try to ensure that students/ pupils will have good access to digital technologies to enhance their learning and will, in return, expect the students I pupils to agree to be responsible users.

Acceptable Use Policy Agreement

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

- I accept that infringements of any of the below rules may result in my being dealt with using the schools Behaviour Policy.

For my own personal safety:

- I understand that the St Margaret Ward Catholic 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 on-line.
- 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 off-line that I have communicated with on-line, 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 on-line.
- I understand that any actions using social media either inside or out of school which affect the wellbeing of staff or students can be dealt with by the academy in accordance with the academy's behaviour policy.

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

- I understand that the school is St Margaret Ward Catholic 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 school systems or devices for on- line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have the permission of a member of staff to do so.
- I will not access, copy, remove or otherwise alter any other users' 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 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 will not use the school network to alter images of students/staff in any way that could be deemed offensive.
- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school/ St Margaret Ward Catholic 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 I 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 I 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.
- I will only use social media sites with permission and at the times that are allowed.

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 in and out of school:

- I understand that St Margaret Ward Catholic 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 as per the St Margaret Ward Catholic Academy's behaviour policy. 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.

If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student / Pupil Acceptable Use Agreement Form

This form relates to the student/ 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 ICT systems.

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

- I use St Margaret Ward Catholic Academy systems and devices (both in and out of school)
- I use my own devices in the *St Margaret Ward Catholic Academy* (when allowed) e.g. Mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school/ St Margaret Ward Catholic Academy in a way that is related to me being a member of this St Margaret Ward Catholic Academy e.g. communicating with other members of the school, accessing school email, VLE, website etc.
- I accept that sanction will be applied as per the school's behaviour policy for misuses of technology.

Name of Student / Pupil	
Group / Class	
Signed	
Date	

School logo and details

Dear Parent/ Carer

ICT including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of e-Safety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their Parent or Carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or Mr P Johnson, the school E-Safety Manager. Please return the bottom section of this form to school for filing.

Pupil and Parent/Carer signature

We have discussed this document and _____(pupil name) agrees to follow the e-Safety rules and to support the safe and responsible use of ICT at St Margaret Ward Catholic Academy.
I accept that sanction(s) will be applied as per the schools behaviour policy for misuses of technology.

Parent/Carer Signature

Pupil Signature

Form

Date

Acceptable Use Agreement: Staff, Governors and Visitors

- ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school E Safety Leader Paul Johnson.
- I will only use the school's email I Internet, Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the network manager Mr. Millward.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the Parent, Carer or Staff Member. Images will not be distributed outside the school network without the permission of the parent/Carer, member of staff or Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature _____ Date___/ ___ / ___

Full Name _____ (Printed)

Job title _____

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive, and a BYOD policy should be in place and reference made within all relevant policies.

- This policy is under constant review and will often be at the discretion of staff in line with curriculum requirements.
- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the St Margaret Ward Catholic Academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy.
- Where pupils use own device for recording images staff will endeavour to ensure images etc. are deleted.
- *BYOD devices may be subjected to* inspections *if used improperly.*

Use of digital and video images

- The development of digital imaging technologies has created significant benefits to learning, allowing staff and students pupil's instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students *I* 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 carers are welcome to take videos and digital images of their children at school 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 I made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital video images.

- Staff and volunteers are allowed to take digital/ video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital/ video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Students must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of students are published on the school website. Once permission is granted it will be the responsibility for parents/ guardians to inform the school of a change in circumstance.

- The initial written permission will be collected as part of the students entry pack. Students' work can only be published with the permission of the student and parents/ Carers.

Staff should inform and educate students */* 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.

In accordance with guidance from the Information Commissioner's Office responsible persons are appointed */* identified;

- Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information Risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage */* cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- 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.
- Remove any images of students or colleagues collected as part of an approved education project are used for that purpose only and deleted as soon as practically possible.
- Regularly change passwords.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.

- The device must be password protected (many memory sticks */* cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g.CD, DVD, Pen Drive or other form of portable media) must be checked for any viruses using school provided anti-virus software before using them.
- Never interfere with any anti-virus software installed on school ICT equipment that you use.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

The school follows Becta guidelines Becta School s- leadership and management- Security - Data handling security guidance for schools (published spring 2009) and the Lo cal Authority guidance documents listed below

Headteacher's Guidance- Data Security in Schools- Dos and Don'ts

- Network Manager/MIS Administrator or Manager Guidance- Data Security in Schools
- Staff Guidance- Data Security in Schools- Dos and Don'ts
  SIRO/IAO Guidance- Data Security in Schools- Dos and Don'ts

The Head, SIRO and Network Manager documents contain advice about identifying information assets including an example of an excel spreadsheet and a brief outline of the school policy that can be displayed at appropriate sites within the school or handed to visitors or guests.

Security

- The School gives relevant staff access to its Management Information System, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Leadership have identified the safety coordinator
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used

Social Media Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual, when publishing any material online. Expectations for teachers professional conduct are set out in Teachers Standards 2012 ·

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues. Training will also include updates on the Academy's code of conduct and will be part of the Academy's induction programme.
Clear reporting guidance, including responsibilities, procedures and sanctions.
Risk assessment, including legal risk School staff should ensure that:
No reference should be made in social media to students, parents *I* carers or school 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 school St Margaret Ward Catholic Academy or local authority
Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The St *Margaret Ward Catholic Academy's* use of social media for professional purposes will be monitored by the academy to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable /Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school/ St Margaret Ward Catholic 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 a school context, either because of the age of the users or the nature of those.

Activities

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Grooming, incitement, arrangement or facilitation of sexual acts against children 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	
	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 school / St Margaret Ward Catholic 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			
On-line gaming (non educational) – Only during non contact time (before, after school and at lunch)		X			
On-line gambling				X	
On-line shopping / commerce		X			
File sharing (educational)		X			
Use of social media (educational – e.g. exam board support groups)			X		
Use of messaging apps (educational)			X		
Use of video broadcasting eg Youtube (educational)	X				

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow the St Margaret Ward Catholic 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 / volunteer 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. o Involvement by Local Authority or national / local organisation (as relevant). o 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:** o incidents of 'grooming' behaviour o the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act o criminally racist material
    - 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 St Margaret Ward Catholic Academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School/ St Margaret Ward Catholic Academy Actions & Sanctions

It is more likely that the school 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 the normal behaviour/procedures.

Students / Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Head teacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion	SMWCA BEHAVOUR POLICY
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X						X
Unauthorised use of non-educational sites during lessons										X
Unauthorised use of mobile phone / digital camera / other mobile device										X
Unauthorised use of social media / messaging apps / personal email										X
Unauthorised downloading or uploading of files										X
Allowing others to access school / St Margaret Ward Catholic Academy network by sharing username and passwords										X
Attempting to access or accessing the school / St Margaret Ward Catholic Academy network, using another student's / pupil's account										X
Attempting to access or accessing the school / St Margaret Ward Catholic Academy network, using the account of a member of staff										X
Corrupting or destroying the data of other users										X

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature										X
Continued infringements of the above, following previous warnings or sanctions										X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school										X
Using proxy sites or other means to subvert the school's / St Margaret Ward Catholic Academy's filtering system										X
Accidentally accessing offensive or pornographic material and failing to report the incident										X
Deliberately accessing or trying to access offensive or pornographic material										X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act										X

Staff

Incidents:	Refer to line manager	Refer to Principal	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X				
Inappropriate personal use of the internet / social media / personal email	X						
Unauthorised downloading or uploading of files	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					
Careless use of personal data eg holding or transferring data in an insecure manner	X						
Deliberate actions to breach data protection or network security rules		X					

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X					
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X					
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X					
Actions which could compromise the staff member's professional standing		X					
Actions which could bring the school / St Margaret Ward Catholic Academy into disrepute or breach the integrity of the ethos of the school / St Margaret Ward Catholic Academy		X					
Using proxy sites or other means to subvert the school's / St Margaret Ward Catholic Academy's filtering system		X					
Accidentally accessing offensive or pornographic material and failing to report the incident	X						
Deliberately accessing or trying to access offensive or pornographic material		X	X				
Breaching copyright or licensing regulations	X						
Continued infringements of the above, following previous warnings or sanctions		X					

Information Asset Owner {IAO}

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff: such as assessment records, medical information and special educational needs data. Please refer to the appendix at the back of this document showing examples of information assets a school may hold. Schools should identify an Information Asset Owner. For example, the school's Management Information System (MIS) should be identified as an asset and should have an Information Asset Owner. In this example the MIS Administrator or Manger could be the IAO.

The role of a IAO is to understand:

- What information is held, and for what purposes.
- What information needs to be protected (e.g. any data that can be linked to an individual, pupil or staff etc. including UPN, Teacher DCSF number etc.) ☐ How information will be amended or added to over time.
- Who has access to the data and why.
- How information is retained and disposed of.

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary School, there may be

several IAOs, whose roles may currently be those of e-safety coordinator, ICT manager or Management Information Systems Administrator or Manager.

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility- whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Extra Policies/Consent Forms

Use of Digital/ Video Images

The use of digital/ video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the GDPR and request parents I carer's permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents I carers are welcome to take videos and digital images of their children at school 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 I made publicly available on social networking sites, nor should parents I carers comment on any activities involving other students in the digital/ video images.

Parents/Carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents *I* carers to agree

Digital *I* Video Images Permission Form

Parent *I* Carers Name

Student *I* Pupil

As the Parent/Carer of the above Student, I agree to the School taking and using digital *I* video images of my child/children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

Yes/No

I agree that if I take digital or video images at SMWCA events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Yes/No

Signed _____

_____

Date _____

Use of Cloud Systems Permission Form

Schools that use Cloud Hosting Services may be required to seek parental permission to set up an account for pupils.

Google Apps for Education services -
https://www.google.com/intl/en_nz/edu/products/productivity-tools/

The school uses Google Apps for Education for pupils/ students and staff. This permission form describes the tools and pupil responsibilities for using these services.

The following services are available to each pupil I student and hosted by Google as part of the school's online presence in Google Apps for Education:

Mail - an individual email account for school use managed by the school

Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments

Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

Sites - an individual and collaborative website creation tool

Using these tools, pupils collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils I students and members of staff.
These services are entirely online and available 2417 from any Internet-connected computer.
Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The school believes that use of the tools significantly adds to your child's educational experience.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Parent / Carers Name

Student / Pupil Name

Yes / No

As the parent / carer of the above *student / pupil,* I agree to my child using the school using Google Apps for Education.

Signed _____

Date _____

Use of Biometric Systems:

See Biometric permission form

Record of reviewing devices *I* internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address *I* device Reason for concern

Conclusion and Action proposed or taken

Password Security

A safe and secure username *I* password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE). Where sensitive data is in use - particularly when accessed on laptops - schools may wish to use more secure forms of authentication e.g. two factor authentication such as the use of hardware tokens and if so should add a relevant section In the policy. Where this is adopted, the policy should state clearly that such items as hardware tokens must be stored separately from the laptop when in transit - to avoid both being lost stolen together

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- All St Margaret Ward Catholic Academy networks and systems will be protected by secure passwords that are regularly changed
- The "master administrator" passwords for the school / St Margaret Ward Catholic Academy systems, used by the technical staff must also be available to the *Principal* or other nominated senior leader and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts.
- Passwords for new users, and replacement passwords for existing users will be allocated by RM. Any changes carried out must be notified to the manager of the password security policy (above).
- All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Users will change their passwords at regular intervals - as described in the staff and student sections below.
- The level of security required may vary for staff and student I pupil accounts and the sens1t1ve nature of any data accessed through that account).
- Requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user (the school will need to decide how this can be managed - possibly by requests being authorized by a line manager for a request by a member of staff or by a member of staff for a request by a pupil I student).

Staff passwords.

All staff users will be provided with a username and password by D Millward

- The password should be a minimum of 8 characters long and must include three of uppercase character, lower case character, a number, special characters must not include proper names or any other personal information about the user that might be known by others.
- The account should be "locked out" following six successive incorrect log-on attempts.
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log- on.
- Passwords shall not be displayed on screen and shall be securely hashed (use of one-way encryption).
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
- Should be changed at least every 60 to 90 days.
- Should not re-used for 6 months and be significantly different from previous p the last four passwords cannot be re-used passwords created by the same user.
- Should be different for different accounts, to ensure that other systems are not put at risk if one is compromised should be different for systems used inside and outside of school.

Student *I* pupil passwords

Primary schools will need to decide at which point they will allocate individual usernames and passwords to pupils. They may choose to use class log-on forks (though increasingly children are using their own passwords to access programmes) Academies need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP. Use by pupils in this way should always be super vised and members of staff should never use a class log on for their own network /Internet access. Academ1es should also consider the implications of using whole class log-ons when providing access to learning environments and applications which may be used outside school

- All users (at KS2 and above) will be provided with a username and password By *Mr Millward who will keep an up to date record of users and their usernames.*
- *Users will be required to change their password every (insert period).*
- Students will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training *I* Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to un-authorised access/data loss. This should apply to even the youngest of users, even if class log-ons are being used

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Pupils I students will be made aware of the school's password policy:

- in lessons (the school should describe how this will take place)
- through the Acceptable Use Agreement

PURPOSE of E-Safety Committee

To provide a consultative group that has wide representation from the School, with responsibility for issues regarding e-safety and the monitoring thee-safety policy including the impact of initiatives. Depending on the size or structure of the school this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Full Governing Body

MEMBERSHIP

1.1 The E-safety committee will seek to include representation from all stakeholders. The composition of the group should include;

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- E-safety coordinator
- ICT Technical Support staff
- Community users (where appropriate)
- Student/ pupil representation- for advice and feedback. Student/ pupil voice is essential in the make- up of the e-safety committee, but students/ pupils would only be expected to take part in committee meetings where deemed relevant.

1.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

1.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

1.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

CHAIRPERSON

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

DURATION OF MEETINGS

Meetings shall be held termly. (A special or extraordinary meeting may be called when and if deemed necessary)

FUNCTIONS

These are to assist the E-safety Coordinator with the following:

- To keep up to date with new developments in the area of E-safety
- To annually review and develop the E-safety policy in line with new technologies and incidents
  To monitor the delivery and impact of the E-safety policy
- To monitor the log of reported E-safety incidents (anonymous) to inform future areas of teaching *I* learning *I* training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of e-safety. This could be carried out through:
- Staff meetings
- Student *I* pupil forums (for advice and feedback)
- Governors meetings
- Surveys/questionnaires for students *I* pupils, parents *I* carers and staff
- Parents evenings
- Website/VLE/Newsletters
- E-safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- Other methods
- To ensure that monitoring is carried out of Internet sites used across the school • To monitor filtering/change control logs (e.g. requests for blocking *I* unblocking sites).
- To monitor the safe use of data across the [school]
- To monitor incidents involving cyberbullying for staff and pupils

AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for St Margaret Ward Catholic Academy have been agreed

Signed by (SLT):

Date:

Date for review: