St. Margaret Clitherow's Catholic Primary School

(Part of St. Oswald's Catholic Voluntary Academy)

Internet Safety Policy

November 2017

Written by:	Mrs Adams
Review Date:	December 2018

Purpose:
In order to create a safe teaching and learning environment, effective policies and procedures which are clearly understood and followed by the whole school community are essential. This Internet Safety Policy sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard adults, children and young people within our school. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate developments within ICT/Computing.

Scope:
This policy is aimed at all staff and for them to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school.

This policy is to be read in conjunction with:

- Data Protection Policy
- Safeguarding Policy
- Mobile Phone Policy
- Digital Images Policy
- Social Networking Policy
- Acceptable Use Policy
- Cyber Bullying Policy
- iPad contract
- SMC Facebook Policy

This policy also has due regard to the following legislation, including but not limited to

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

This policy also has regard for the following statutory guidance

- DfE (2016) 'Keeping Children Safe in Education

Roles and Responsibilities:

The Local Management Board must ensure that this policy is implemented and that both current and new employees have access to, and are made aware of, this policy.

Headteachers/Line Managers must be fully aware of this policy and ensure that they and all employees are aware of the policy and their own responsibilities.

All users of St. Oswald's Catholic Academy Trust computing facilities whether they are staff, students, supply staff, or a visitor with temporary access privileges to familiarise themselves, adhere to this document and review it on a regular basis. All users must behave responsibly and professionally at all times in connection with the use of the Academy Trust's ICT facilities and must comply with this policy and co-operate fully with the academy's management in ensuring the implementation of this policy.

Advice from Human Resources can be sought where necessary, particularly where disciplinary procedures may need to be instigated.

Head Teacher:
The Head Teacher has the ultimate responsibility of ensuring that all policies and practices are embedded and monitored. At St Margaret Clitherow's (SMC) either Mrs N Jamalizadeh or in her absence Miss C McNicholas will be responsible for the strategic leadership within school.

Computing Subject Leader:
Mrs H Adams is the Computing Subject Lead and will take responsibility for

- Monitoring the provision of Internet Safety within school and reporting to the Head Teacher
- Ensuring that all staff members are aware of the procedures for reporting incidents and inappropriate Internet use, either by pupils or staff
- Ensuring that cyber bullying incidents are reported in accordance with the schools policy (using CPOMS)
- Act as first point of contact for any staff needing advice on Internet Safety matters
- Regularly reviewing this Internet Safety Policy and making changes as necessary (e.g. as technology changes and advances)
- Producing an annual Internet Safety Calendar making staff aware of Internet Safety issues throughout the year.

St Margaret Clitherow's understands the importance of using the Internet as a teaching tool in raising standards, promoting pupil achievement and enhancing teaching and learning. The school also understands that in accessing the Internet individuals are especially vulnerable to a number of risks which may be physically or emotionally harmful including

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to or loss of personal information
- Access to unsuitable online videos or games
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individuals consent or knowledge

Though these risks cannot ever be truly eradicated SMC aims to minimise their damage effects by monitoring and filtering

St. Oswald's Catholic Academy Trust IT Department may monitor the use of any ICT System including Internet and Email activity occurring on Academy equipment or accounts at any time. Internet access is logged and may be viewed by any authorised staff as listed in Appendix A including Head Teachers, Network Manager and the Police if the need to do so arises.

St. Oswald's Catholic Voluntary Academy currently employs both Web and Email filtering software to limit access to sites on the Internet and for the scanning of email for virus protection. If St. Oswald's Catholic Academy Trust discovers activities which do not comply with current applicable law or Academy policy, records retrieved may be used to document the wrongful content in accordance with due process.

Staff are responsible for defining appropriate Internet access levels for the students in their lesson, subject or year group and setting the appropriate internet access before students are allowed to access the Internet. Students must be given clear guidance on what sites and web searches are appropriate before accessing the internet.

As online resources frequently change, staff must first check that any online resources used is still suitable prior to use or display on any whiteboard, touchscreen, or other presentation screen. You are strongly advised to download any content rather than to depend upon an internet source.

In the unlikely event of any inappropriate material passing the internet filters, immediately ensure no one can see the content i.e. by locking the device or turn off the screen. Do not turn off the device. Immediately report the incident to the Head Teacher and Network Manager for further action.

On occasion particular planned curricular activities require students to access or research educational material that may be deemed inappropriate, for example war and racial issues, etc. Any such access must be pre-planned and recorded so that it can be justified if required.

Disclaimer

St. Oswald's Catholic Academy Trust assumes no liability for any direct or indirect damages arising from the user's connection to the Internet. St. Oswald's Catholic Academy Trust is not responsible for the accuracy of information found on the Internet and only facilitates the accessing and dissemination of information through its systems. Users are solely responsible for any material that they access and disseminate through the Internet.

Internet Safety Education:

Educating Pupils

- An Internet Safety programme has been established and will be taught across the curriculum on a regular basis, ensuring pupils are aware of the safe use of technology both inside and outside of the school.
- Pupils are taught, in an age appropriate way, the importance of Internet Safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of the website
- Pupils are taught to acknowledge the information they access online in order to avoid copyright infringement and/or plagiarism

- Clear guidance on the rules of Internet use and will be presented in all classrooms Appendix B and C
- Pupils are instructed to report any suspicious use of the Internet and digital devices
- The school will hold Internet Safety events, such as Safer Internet Day and Anti-Bullying Week, to promote online safety

Educating staff

- Staff are given an e-safety calendar at the beginning of the year with activities and Internet safety links for them to use in their teaching
- Staff will undergo regular Internet Safety training so they are aware of current e-safety issues and any changes to the provision of e-safety
- All staff will employ methods of good practice and act as role models for pupils when using the Internet and other digital devices
- Staff will only use sites which are deemed appropriate for use with children
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism
- The Computing Lead will act as first point of contact for staff requiring e-safety advice

Educating Parents

- Internet Safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and Facebook page
- Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any Internet safety related concerns

Internet Safety Control Measures

- Internet Access will only be authorised once parents and pupils have returned the signed consent form in line with St Oswald's Academy Acceptable Use Agreement (See appendix D)
- A record will be kept in the school office of all pupils who have been granted Internet access
- All users in KS2 will be provided with usernames and passwords, and are advised to keep these confidential to avoid any other pupils using their login details.
- Management systems will be in place to allow System Admin to control workstations and monitor pupils' activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- The governing body will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable

restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the Head Teacher
- All school systems will be protected by up-to-date virus software.
- Visitors are prohibited from connecting any device to the Academy Trust Network. A segregated guest wireless network is provided for visitor access to the Internet if required. The same monitoring policy applies to the guest Wi-Fi.

Social Networking

- Use of social media on behalf of the school will be conducted following the processes outlined in our Social Networking Policy
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason e.g. a teaching purpose, this will be monitored and controlled by staff at all times and must be first authorised by the Head Teacher
- Pupils are regularly educated on the implications of posting personal data online outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
  Staff are not permitted to publish comments about the school.

Published Content on the school website and Images (to be read with St Oswald's Digital Images Policy)

- The Head Teacher will be responsible for the overall content of the school website and will ensure the content is appropriate and accurate
- Contact details on the website will include the phone number and email address of the school – no personal details of staff or pupils will be published
- Images will not be used with any part of a child's name
- Staff are able to take pictures but they must do so in accordance with school policies in terms of the sharing and distribution of such. **Staff will not take pictures with their personal equipment**

Reporting Misuse

St Margaret Clitherow's and St Oswald's Academy Trust have clearly defined what is classed as inappropriate behaviour in the Acceptable Use Policies, ensuring all pupils and staff members are aware of what behaviour is expected of them.

Inappropriate activities are discussed and the reasoning behind prohibiting activities due to Internet safety concerns are explained to pupils as part of the curriculum in order to promote sensible Internet use.

Misuse by pupils

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to Internet use in line with SMC Behaviour Policy
- Any instances of misuse will be immediately reported using CPOMS
- Any pupil found who does not adhere to the Acceptable Use Agreement and is found wilfully misusing the Internet will have their Internet use in school suspended with a letter sent to parents explaining why
- Complaints of a child protection nature, such as when a child is found to be accessing extremist material shall be dealt with in accordance with the Safeguarding policy and Prevent Training

Misuse by Staff

- Any misuse of the Internet by a member of staff should immediately be reported to the Head Teacher
- The Head Teacher will deal with such incidents in accordance with the Allegations of Abuse against Staff Policy and may decide to take disciplinary action against the member of staff
- The Head Teacher will decide if it is appropriate to notify the police of the action taken against a member of staff

Use of Illegal material

- In the event that illegal material is found on the school's network, or the evidence suggests that illegal material has been accessed, the police will be contacted
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK
- If a child protection incident is suspected the school's child protection procedure will be followed. The DSL/Head Teacher will be informed and the police contacted

Failure to Comply

Violations of this policy will be treated like other allegations of inappropriate behaviour at St. Oswald's Catholic Academy Trust. Allegations of misconduct will be dealt with according to current behavioural procedures, this may include, but is not limited to, one or more of the following:

1. Temporary or permanent revocation of access to some or all computing and networking resources and facilities.
2. Disciplinary action according to applicable St. Oswald's Catholic Academy Trust policies.

3. In extreme cases legal action according to applicable laws.

We encourage you to use your Email, Internet access, computer account and all other ICT services responsibly. Should you have any questions regarding this Acceptable Use Policy, feel free to contact, Mrs Adams, (SMC Computing Lead) the Academy's ICT Department or SMC Senior Leadership Team.

Appendix A – Designated System Admins

There are many different ICT Systems in use across the Academy Trust the following is a list of named systems admins for each system.

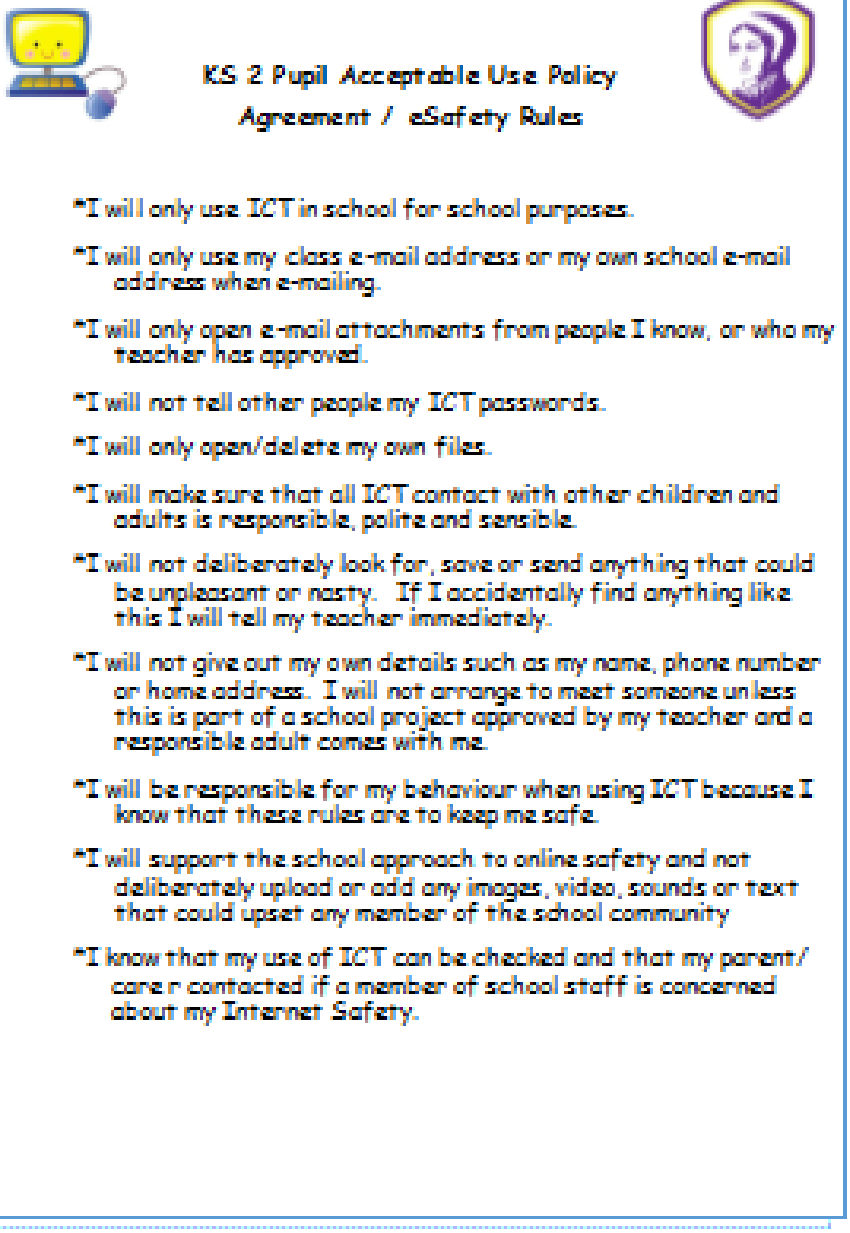
System	Named Person With Admin Access
Network Servers and Account Control	All Sites D Jackson All Sites N Potter All Sites A Holian
Office 365 Email System	All Sites D Jackson All Sites N Potter All Sites A Holian SMC Only H Adams
Firewall and WebFilter	All Sites D Jackson All Sites N Potter All Sites A Holian
CPOMS	SMC H Adams All Sites J Benson
SIMS.NET	All Sites D Jackson All Sites N Potter All Sites A Holian

Appendix B – Key Stage 1 and EYFS Online safety Poster

AUP KS1 and EYFS 2016.pub

Appendix C – Key Stage 2 Online safety Poster

AUP KS 2.pub



KS 2 Pupil Acceptable Use Policy
Agreement / eSafety Rules

- "I will only use ICT in school for school purposes.
- "I will only use my class e-mail address or my own school e-mail address when e-mailing.
- "I will only open e-mail attachments from people I know, or who my teacher has approved.
- "I will not tell other people my ICT passwords.
- "I will only open/delete my own files.
- "I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- "I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- "I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- "I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- "I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- "I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my Internet Safety.

Appendix D – Acceptable Use Policy for Students

ST OSWALD'S
CATHOLIC ACADEMY TRUST

ICT Systems Acceptable Use Policy for Students

To be Signed and Returned to the Academy School Office

I have read and agree to comply with all parts of the ICT Systems Acceptable Use Policy and understand that any unlawful or unsafe behaviour could lead to appropriate legal or disciplinary action being taken.

Academy Trust School _____

Students Name_____

Signed Name _____

Date _____