Romero Catholic Academy Trust

All Saints'
Roman Catholic High School,
A Voluntary Academy

Headteacher: Mr Brian McNally, MA, BSc (Hons), NPQH.
Address: Haslingden Road, Rawtenstall, Rossendale, Lancashire, BB4 6SJ
Telephone: 01706 213 693
Email: office@allsaintshigh.lancs.sch.uk
Website: www.allsaintshigh.lancs.sch.uk

All Saints' Roman Catholic High School, A Voluntary Academy

part of
Romero Catholic Academy Trust

Luceat Lux Vestra

Online Safety (E-Safety) Policy

Updated: Spring 2021
To be reviewed: Spring 2024

Responsibility of: ICT Curriculum Leader
Approved by: Quality Of Education Committee

Policy Approval:

25/03/2021

Signature of Headteacher — Date

25/03/2021

Signature of Committee Chair/Vice-Chair — Date

Mission Statement

All Saints' is a school where the Catholic faith is taught, lived and celebrated.

We will educate the whole person spiritually, morally and intellectually.

We embrace Catholic values in all we do and in all our relationships.

We will identify and cater for the individual student's needs and prepare them for responsible participation in society.

Our aim is to follow Christ's teaching, as found in the Gospels, in everything we do.

ONLINE SAFETY (E-SAFETY) POLICY

Introduction and Aims

The purpose of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet. This includes the misuse of ICT, including mobile phones, which has become an increasingly prolific area of safeguarding in the last few years.

This policy should be read alongside the school's Acceptable Internet Use for Staff and Volunteers policy, and the policy on Social Networking.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically Anti-Bullying, Behaviour, Child Protection and Mobile Phone Use.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Scope

This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents/carers and visitors and community users) who have access to and are users of school IT systems, both in and out of school. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school. 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 Behaviour Policy.

Roles & Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

There is an appendix which relates in more detail solely to the use of social networking sites and other forms of social media by staff.

Governors

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. A member of the Governing Body, has taken on the role of Child Safety Governor. The role of this Governor will include:

- Meetings with the SLT link for Safeguarding
- Reporting to relevant Governors and/or committee(s) meetings.

Headteacher and Senior Leaders

The Headteacher is responsible for ensuring:

- The safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety may be delegated to the Safeguarding link E-safety co-ordinator
- Adequate training is provided
- Effective monitoring systems are set up
- That relevant procedure in the event of an e-safety allegation are known and understood. The Headteacher and another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- Establishing and reviewing the school e-safety policies and documents (in conjunction with e-safety co-ordinator)
- The school's Designated Senior Leader on Child Protection should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

Designated Safeguarding Lead

Responsibility for e-safety issues and has a leading role in:

- Leads the e-safety committee
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / 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
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- Attends relevant meeting / committee of Governors / Directors
- Reports regularly to Senior Leadership Team.
- Liaising with staff, the LA, ICT Technical staff, Safeguarding Governor and SLT on all issues related to e-safety;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- Co-ordinating and reviewing e-safety education programme in school

ICT Coordinator

The ICT Coordinator is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets e-safety technical requirements
- The school's password policy is adhered to
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Co-ordinator keeps up to date with e-safety technical information

- The use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the Safeguarding link and/or SLT for investigation/action/sanction.

Teaching & Support Staff

In addition to elements covered in the Staff Accessible Usage Policy (AUP), all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Usage Policy (AUP)
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school's e-safety and acceptable usage policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- In lessons where Internet use is pre-planned, 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.

Students (to an age appropriate level)

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues, through newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website
- Endorsing (by signature) the Pupil Acceptable Usage Policy.
- Accessing the school website in accordance with the relevant school Acceptable Usage Policy.

Community Users

Community Users who access school ICT systems/website/Learning Platform as part of the
Extended School provision will be expected to sign a Volunteer User AUP (see Appendix 6) before being provided with access to school systems.

Education and Training

E-safety education will be provided in the following ways:

- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Students are helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school
- Staff should act as good role models in their use of ICT, the Internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that 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
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) 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 - Acceptable Usage Policy

- **Parents/carers** will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules
- **Staff and regular visitors** to the school have an AUP that they must read through and sign to indicate understanding of the rules.

Copyright

- Students to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this.
- Students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

Staff Training

- Safeguarding link ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- A planned programme of e-safety training is available to all **staff**.
- All new **staff** receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy, Acceptable Usage and Child Protection Policies.
- The **Safeguarding link** will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.

Technical – infrastructure / equipment, filtering and monitoring

The school 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 need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School / Academy technical systems will be managed in ways that ensure that the school 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 school technical systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The “administrator” passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept in the school safe)

- The Headteacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes

- School staff regularly monitor 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 for users to report any actual / potential technical incident / security breach to a member of staff, who will then ensure this is passed onto a member of the e-safety group
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. 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" (eg trainee teachers, supply teachers, visitors) onto the school systems
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / 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

Commmunication

Email

- Digital communications with pupils (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official school systems (see staff guidance in child protection policy).
- Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses.
- Staff can use their own email in school (before, after school and during lunchtimes when not working with children) – but not for contact with parents/ pupils.

Mobile Phones

- **School** mobile phones should only be used to contact parents/carers/students when on school business with students off site.
- **Staff** should not be using personal mobile phones in school during working hours when in contact with children.
- Students should adhere to the rules and guidelines set out in the Parent Handbook regarding mobile phone use in school.

Social Networking Sites

Young people will not be allowed on social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- **Staff** should not access social networking sites for personal use on school equipment in school or at home. Staff should access sites using personal equipment.
- **Staff** users should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site or blog**.**
- **Staff** should be aware the school will investigate use of social networking if it impacts on the reputation of the school.
- **Students/Parents/carers** should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.
- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.
- Students in the KS3 curriculum will be taught about e-safety on social networking sites as we accept some may use it outside of school.

Microsoft TEAMS - Rational

School to family interactions have had to be made at a distance since the Covid-19 outbreak and require teachers and students to adapt normal classroom routines to the online world. It is an expectation the normal high levels of behaviour expected when in school will remain in place at all times when interacting with the school from home.

Digital technologies have become integral to the lives of children and young people. These technologies are powerful tools which open up new opportunities including the offer of pastoral and academic support for students. Technologies and digital platforms such as Microsoft Teams can provide opportunities for discussion, promote creativity and stimulate awareness of contextualised subjects to provide effective support for pupils based on their individual pastoral and academic needs.

Young people should always have an entitlement to safe internet access. This Policy is intended to ensure that young people will be responsible users and stay safe while using the internet and other digital technologies to interact with All Saints High School. That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

All Saints Catholic High School staff will primarily use Microsoft Teams as a communication tool to support students in a pastoral manner and the platform can also be used for academic purposes in case of school closure and for extra intervention for students.

Gaining access to Microsoft Teams

To gain access to Microsoft Teams every student will be provided with an email address and a password. The email address will act as the student's Office 365 log-on name. Once logged on students can access the Teams icon within this software.

The email address will also allow students to access and use the school email system which can also be found on the Office 365 homepage. Both platforms are monitored and neither should be considered 'private' by students. Students are responsible for their own accounts and are expected to follow the Online Safety rules taught in lessons when interacting on Microsoft Teams including (but not exclusive to):

- Never revealing private information including date of birth, home addresses or contact details.
- Never distribute images of themselves of others via Microsoft Teams.
- Using appropriate words and actions when participating in calls and chats.

Students are strongly advised never to share their log-on name or password with anybody other than their trusted adults within their home environment.

Microsoft Teams in a 'Live' format

'Live' interactions to support students will always be initiated by a staff member who will make contact with students prior to the interaction starting to advise a start date and time. Staff will inform all students when the interaction has finished, and all students will log off Microsoft Teams immediately to allow the staff member to close the call.

Student behaviour when participating within a 'Live' interaction will mirror normal classroom behaviour. Students will be expected to:

- Respect all participants by allowing others to share their viewpoint in a safe environment.
- Respond to questions or tasks from staff members in an appropriate way.
- Attempt all tasks in a positive manner.
- Engage with enthusiasm when collaborating virtually with class members.

Remote Interactions using Microsoft Teams

For Microsoft Teams to be used effectively and safely, students must agree to the following points:

- Students must not use Microsoft Teams to call, chat or set up groups between each other or with any staff and parents.
- Students must not attempt to start or record a meeting.
- Students must not share any resources, recorded videos, PowerPoints, assemblies or other materials uploaded by staff or other students within or outside of All Saints Teams accounts.
- Students must blur their backgrounds (if this facility is available) when they are participating in a meeting which involves switching on their camera.
- Students must think carefully about what acceptable language with regards is to what they say, type or post when using Microsoft Teams. This includes the use of emoji's and images.
- Students must hang up at the end of the interaction or when instructed to do so.

Digital Images

- The school record of parental permissions granted/not granted must be adhered to when taking images of our students. A list is published to all staff on a termly basis, but can also be obtained from the data office or the child protection officers in school.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Headteacher.
- Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has an active website and social media accounts which are used to inform, publicise school events and celebrate and share the achievement of students.

Removable Data Storage Devices

- Anything that contains personal information about staff or pupils should not be on any device that is not password protected.

- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks.

- Students should not bring their own removable data storage devices into school unless asked to do so by a member of staff.

Websites

- In lessons where Internet use is pre-planned, 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.
- Staff will preview any recommended sites before use.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. **Parents** will be advised to supervise any further research.
- **All** users must observe copyright of materials published on the Internet.
- Teachers will carry out a risk assessment regarding which students are allowed access to the internet with minimal supervision. Minimal supervision means regular

checking of the students on the internet by the member of staff setting the task. All staff are aware that if they pass students working on the internet that they have a role in checking what is being viewed. Students are also aware that all internet use at school is tracked and logged.

- The school only allows the E-Safety Co-ordinator, ICT co-ordinator, Network Manager and SLT to access to Internet logs.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file

Students

- Inform staff immediately if passwords are traced or forgotten.

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Headteacher, Network Manager or ICT Co-ordinator.
- Students should not bring in their own equipment unless asked to do so by a member of staff.

Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment without the specific permission of the Headteacher, Network Manager or the ICT Co-ordinator.
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- All should ensure any screens are locked before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring

All use of the school's Internet access is logged and monitored. Whenever any inappropriate use is detected it will be followed up by the E-Safety Co-ordinator, Student Managers, Progress Leaders or members of the Senior Leadership Team depending on the severity of the incident.

- Safeguarding link and ICT Co-ordinator will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering systems
- Any member of staff employed by the school who comes across an e-safety issue does not investigate any further but immediately reports it to the e-safety co-ordinator and impounds the equipment. This is part of the school safeguarding protocol. (If the concern involves the E-Safety co-ordinator then the member of staff should report the issue to the Headteacher).

Incident Reporting

Any e-safety incidents must immediately be reported to the Headteacher (if a member of staff) or the Safeguarding link (if a student) who will investigate further following e-safety and safeguarding policies and guidance.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. Listed in Appendix 2 are the responses that will be made to any apparent or actual incidents of misuse. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the flow chart should be consulted. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer. 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 normal behaviour/disciplinary procedures as follows (Appendix 3 for students and Appendix 4 for staff respectively).

Appendix 1

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

		Staff and other adults					Students and young people			
Communication Technologies		Permitted	Permitted at certain times	Permitted for named staff	Not Permitted		Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones May be brought to school		✓					✓			
Mobile phones used in lessons			✓							✓
Use of mobile phones in social time		✓							✓	
Taking photographs on mobile devices			✓						✓	
Use of PDAs and other educational mobile devices		✓					✓			
Use of school email for personal emails			✓							✓
Social use of chat rooms/facilities										✓
Use of social network sites			✓						✓	
Use of educational		✓					✓			

blogs									

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access or web portal).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person (in accordance with the school policy) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, chat, Learning Platform etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Appendix 2

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 and all other ICT 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 certain internet usage as follows. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Promotion of racial or religious hatred					✓
Threatening behaviour, including promotion of physical violence or mental harm					✓
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				✓	
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary				✓	

licensing permissions					
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	
On-line gaming (educational)		✓			
On-line gaming (non- educational)				✓	
On-line gambling				✓	
On-line shopping / commerce			✓		
File sharing			✓		
Use of social networking sites			✓		
Downloading video broadcasting e.g. Youtube	✓				
Uploading to video broadcast e.g. Youtube			✓		

Appendix 3

Incident involving students	**Teacher to use school behaviour policy to deal with**	**Refer to Safeguarding SLT Link**	**Refer to police**	**Refer to technical support staff for action re security/filtering etc**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities**).**		✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓			✓
Unauthorised use of mobile phone/ digital camera/ other handheld device.	✓			
Unauthorised use of social networking/ instant messaging/ personal email	✓	✓		✓
Unauthorised downloading or uploading of files		✓		✓
Allowing others to access school network by sharing username and passwords		✓		✓
Attempting to access or accessing the school network, using another student's account		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff		✓		✓
Corrupting or destroying the data of other users		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓		✓
Continued infringements of the above, following previous			Community	

warnings or sanctions		✓	Police Officer referral	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓

The guidance in this policy should be implemented with cross reference to the School's Child Protection, Anti-Bullying and Behaviour Policies. Note, attempts have been made to synchronise guidance and sanctions.

Appendix 4

Incidents involving members of staff	**Refer to the Headteacher** ***See below**	**Refer to technical support staff for action re filtering, security etc**	**Referral to Safeguarding SLT LInk** **Potential Disciplinary Action**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓
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.	✓	✓	✓
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓		✓
Deliberate actions to breach data protection or network security rules	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ pupils	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of			

the school	✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓		✓

***In event of breaches of policy by the Headteacher, refer to the Chair of Governors.**

Appendix 5

Acceptable Internet Use Policy – Students

This document is a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school IT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will only use my personal hand held devices (e.g. mobile phone/ipod) in school at times that are permitted. When using my own devices I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet 'on-line friends' unless I take an adult.
- I will not take, or distribute, images of anyone without their permission.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

Signed ……..

Date …….

Appendix 6
Acceptable Internet Use Policy – Staff and Volunteers

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

This policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

- All Saints ICT systems users are protected from accidental or deliberate misuse that could put the security of the systems or users at risk.

- Staff are protected from potential risk in their use of ICT in their everyday work.

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

Responsible Use Agreement

I understand that I must use All Saints 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 recognise the value of the use of ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of ICT.

For my professional and personal safety:

- I understand that the school will monitor my use of ICT systems, email and other digital

  communications.
- I understand the rules set out in this agreement also apply to the use of the school ICT

  systems (e.g. laptops, email, Learning Platform etc.) out of the school.
- I understand that the school ICT systems are primarily intended for educational use and that I

  will only use systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username and password to anyone else, nor will I try to use any other

person's username and password.

- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the appropriate person (see policy flowcharts).

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images.
- I will only communicate with student and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

All Saints and the Local Authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school's equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse

  images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems .

- I will not (unless I have permission) make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment.

- Where personal data is transferred outside the secure LA network, it must be encrypted.

- I understand that data protection policy requires that any staff or learner data to which I have

  access, will be kept private and confidential, except when it is deemed necessary that I am
  required by law or by policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software

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

- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies

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

- I understand that this Acceptable Use Policy applies not only to my work and use of All Saints ICT equipment in school, but also applies to my use of school ICT systems and equipment out of the school and my use of personal equipment in the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and, in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the All Saints' ICT systems within these guidelines.

SAFEGUARDING
I have read "Keeping Children Safe In Education Part 1".

I have read the Child Protection Policy.

Staff/Volunteer

Name ……..

Signed …….

Date ……..

Appendix 7

LANCASHIRE COUNTY COUNCIL
DIRECTORATE FOR CHILDREN AND YOUNG PEOPLE

MODEL POLICY ON THE USE OF SOCIAL NETWORKING SITES AND OTHER FORMS OF SOCIAL MEDIA (APRIL 2015)

The Governing Body of All Saints' Catholic High School adopted this policy on 1st July 2015. The policy will be reviewed on an annual basis.

This Policy has been developed in consultation with the recognised Trade Unions and professional Associations.

1. PURPOSE

This Policy sets out the school's position regarding the use of social networking sites and other forms of social media. The aim of the document is to ensure that all employees are fully aware of the risks associated with using such sites and their responsibilities with regards to the safeguarding and protection of both children and themselves.

2. APPLICATION

This Policy applies to all staff employed in delegated schools and those Teachers employed in Centrally Managed Services.

3. BACKGROUND

3.1 The use of social networking sites such as Facebook, Bebo, Twitter and MySpace has over recent years become the primary form of communication between friends and family. In addition there are many other sites which allow people to publish their own pictures, text and videos such as YouTube and Instagram.

3.2 It would not be reasonable to expect or instruct employees not to use these sites which, if used with caution, should have no impact whatsoever on their role in school. Indeed, appropriate use of some sites may also have professional benefits. For example many schools now use sites such as Facebook and Twitter as a means to enhance parental engagement.

3.3 It is now widely acknowledged that use of such sites does not provide a completely private platform for personal communications. Even when utilised sensibly and with caution employees are vulnerable to their personal details being exposed to a wider audience than they might otherwise have intended. One example of this is when photographs and comments are published by others

without the employees consent or knowledge which may portray the employee in a manner which is not conducive to their role in school.

3.4 Difficulties arise when staff utilise these sites and they do not have the relevant knowledge or skills to ensure adequate security and privacy settings. In addition there are some cases when employees deliberately use these sites to communicate with and/or form inappropriate relationships with children and young people.

4. GUIDANCE AND ADVICE

4.1 Employees who choose to make use of social networking site/media should be advised as follows:-

(i) That they should not access these sites for personal use during working hours;

(ii) That they familiarise themselves with the site's 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended;

(iii) That they do not conduct or portray themselves in a manner which may:-

- bring the school into disrepute;
- lead to valid parental complaints;
- be deemed as derogatory towards the school and/or it's employees;
- be deemed as derogatory towards pupils and/or parents and carers;
- bring into question their appropriateness to work with children and young people.

(iv) That they do not form on-line 'friendships' or enter into communication with *parents/carers and pupils as this could lead to professional relationships being compromised.

(v) On-line friendships and communication with former pupils should be strongly discouraged particularly if the pupils are under the age of 18 years.

*(*In some cases employees in schools/services are related to parents/carers and/or pupils or may have formed on-line friendships with them prior to them becoming parents/carers and/or pupils of the school/service. In these cases employees should be advised that the nature of such relationships has changed and that they need to be aware of the risks of continuing with this method of contact. They should be advised that such contact is contradictory to this Policy and as such they are potentially placing themselves at risk of formal action being taken under the school's Disciplinary Procedure*.)

4.2 Schools should not access social networking sites in order to 'vet' prospective employees. Such practice could potentially create an un-level playing field and lead to claims of discrimination if for example the selection panel were to

discover a candidate held a protective characteristic as defined by the Equality Act.

5. SAFEGUARDING ISSUES

Communicating with both current and former pupils via social networking sites or via other non-school related mechanisms such as personal e-mails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

The Department for Education document 'Guidance for Safer Working Practices for Adults Working with Children and Young people in Educational Settings (March 2009) states:-

12. Communication with Pupils *(including the Use of Technology)*	
In order to make best use of the many educational and social benefits of new technologies, pupils need opportunities to use and explore the digital world, using multiple devices from multiple locations. It is now recognised that that e.safety risks are posed more by behaviours and values than the technology itself. Adults working in this area must therefore ensure that they establish safe and responsible online behaviours. This means working to local and national guidelines on acceptable user policies. These detail the way in which new and emerging technologies may and may not be used and identify the sanctions for misuse. Learning Platforms are now widely established and clear agreement by all parties about acceptable and responsible use is essential.	*This means that schools/services should:* *- have in place an Acceptable Use* *policy (AUP)* *- continually self-review e.safety* *policies in the light of new and* *emerging technologies* *- have a communication policy which* *specifies acceptable and* *permissible modes of communication*
Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be	

appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny. Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used in accordance with the school/service's policy. Further information can be obtained from http://www.education.gov.uk/	*This means that adults should:* *- ensure that personal social networking sites are set at private and pupils are never listed as approved contacts* *- never use or access social networking sites of pupils.* *- not give their personal contact details to pupils, including their mobile telephone number* *- only use equipment e.g. mobile phones, provided by school/service to communicate with children, making sure that parents have given permission for this form of communication to be used* *- only make contact with children for professional reasons and in accordance with any*

	school/service *policy* *- recognise that text messaging should* *only be used as part of an agreed* *protocol and when other forms of* *communication are not possible* *not use internet or web-based* *communication channels to send* *personal messages to a child/young person*

6. RECOMMENDATIONS

(i) That this policy document is shared with all staff who come into contact with children and young people, that it is retained in Staff Handbooks and that it is specifically referred to when inducting new members of staff into your school/service.

(ii) That appropriate links are made to this document with your school/services Acceptable Use Policy

(iii) That employees are encouraged to consider any guidance issued by their professional association/trade union concerning the use of social networking sites

(iv) That employees are informed that disciplinary action may be taken in relation to those members of staff who conduct themselves in a way which is contrary to the advice and guidance outlined in this Policy. If such conduct is deemed to amount to gross misconduct this may lead to dismissal.