SACRED HEART OF MARY GIRLS' SCHOOL

ONLINE SAFETY POLICY

Policy adopted	**July 2022**	
SLT Member Responsible	**Mrs C Raper**	
To be reviewed	**Every 2 Years**	
Date of next review	**July 2024**	
Headteacher	**Ms V Qurrey**	**Date: 12 July 2022**

ONLINE SAFETY POLICY

1. Introduction

Sacred Heart of Mary is a Catholic Community that aims to carry out its mission "Ut Vitam Habeant" - that they may have life, Life to the Full.

This policy aims to help all stakeholders live out the Gospel values as given by Jesus Christ in The Beatitudes.

These reveal the goal of human existence and are the objective values as given by Christ;

- Forgiveness & Mercy
- Truth & Justice
- Tolerance & Peace
- Dignity & Compassion
- Purity & Holiness
- Humility & Gentleness
- Faithfulness & Integrity
- Preferential Option for the Poor & Vulnerable
- Sanctity of Life & Care for God's Creation
- Solidarity & The Common Good
- Charity & Subsidiarity
- Distributism & Social Justice

Since the foundation of Sacred Heart of Mary Girls' School by the Sacred Heart of Mary Sisters these values have formed the basis of all relationships.

All adults that have chosen to work and oversee this community must ensure that they fulfil their mission of Catholic education by displaying, modelling and promoting these values.

All who work in or oversee a Catholic school must conduct themselves in a way which does not conflict with the "precept" and "tenets" of the Catholic Church and are bound by their contractual obligations "not to do anything in any way detrimental or prejudicial to the interest of the Catholic character of the school".

Every individual in a Catholic school have the entitlement to be treated with the love, respect and dignity that comes from being a child of God, with the face of Christ.

This policy has expectations for all that are rooted in these Gospel Values and conform to the teaching of the Catholic Church. The implementation of all school policies should demonstrate the importance of personal responsibility and the need for justice but also facilitate healing and reconciliation.

The Sacred Heart of Mary Girls' School, as a Catholic learning organisation, believes that people are the school's most valuable resource. We appreciate each member of the school community as a unique individual with God-given gifts that must be exploited to the full if the school is to adhere to its Mission and aims.

It is essential, therefore, that all staff and governors have access to effective Performance Management and professional development activities appropriate to their needs in order for them to use the gifts they have been given to good purpose.

2. Aims

The Sacred Heart of Mary Girls' School (the School) aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

3. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:
Teaching online safety in schools
Preventing and tackling bullying
Cyberbullying: Advice for headteachers and school staff
Relationships and sex education
Searching, screening and confiscation
It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
The policy also takes into account the National Curriculum computing programmes of study.
This policy complies with our funding agreement and articles of association.

4. Roles and responsibilities

4.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The governor who oversees online safety is the Safeguarding Governor.The Safeguarding governor meets termly with the DSL where online safety and related issues are discussed.
All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

4.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, Network manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged via MyConcern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

4.4 The Network manager

The Network manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged via MyConcern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

4.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged via MyConcern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

4.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

4.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

5. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them

- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.
Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

6. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. Cyber-bullying

7.1 Definition
Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school 'Child Protection and Safeguarding Policy' and 'Behaviour Policy')

7.2 Preventing and addressing cyber-bullying
To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups.
Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
The school also shares information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been

spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices
School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police* via the School Safety team

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.
Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

8. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1/ 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
More information is set out in the acceptable use agreements in appendices 1 and 2.

9. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school
- Examinations

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).
Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.This includes smart watches. No watches or mobile phones are allowed in examinations.

10. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 12 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 2.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager.

11. Use of social media

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. As stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

All members of the School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

We will control pupil and staff access to social media whilst using the school network and wi-fi.

Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member of the School community on social media, should be reported to the DSL and will be managed in accordance with relevant Policies.

11.1 Staff Personal Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policies.

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school.

Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites
- Being aware of location sharing services
- Opting out of public listings on social networking sites
- Logging out of accounts after use
- Keeping passwords safe and confidential
- Ensuring staff do not represent their personal views as that of the school

Members of staff are encouraged not to identify themselves as employees of the School on their personal social networking accounts; this is to prevent information on these sites from being linked with the school, and to safeguard the privacy of staff members.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the DSL and/or the Headteacher immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with pupils and parents/carers
Parents should be contacted only via school phones and using school emails
All members of staff are advised not to communicate with or add as 'friends' any current pupils or their family members via any personal social media sites, applications or profiles.
Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the DSL and/or the Headteacher.
Any communication from pupils and parents received on personal social media accounts will be reported to the DSL and/or The Headteacher.

11.2 Pupils' Personal Use of Social Media
Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms and not encourage or condone underage use.
Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
Any concerns regarding a pupil's use of social media will be dealt with in accordance with existing policies. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Pupils will be advised:
- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present
- To use safe passwords
- To use social media sites which are appropriate for their age and abilities
- How to block and report unwanted communications

- How to report concerns both within the setting and externally

11.3 Official Use of Social Media
The School has official social media accounts. The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes. The official use of social media as a communication tool has been formally risk assessed and approved by the DSL and/or Headteacher. Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
Staff use setting-provided email addresses to register for and manage any official social media channels.
Official social media sites are suitably protected and, where possible, run and linked to our website.
Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by the Headteacher.
Official social media use will be conducted in line with existing policies.
All communication on official social media platforms will be clear, transparent and open to scrutiny.
Any social media from the House Teams has to be approved by the Head of House.
Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community. Written parental consent will be obtained, as required.
Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
Any official social media activity involving pupils will be moderated.
We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations
Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.
If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
- always be professional and aware they are an ambassador for the school
- disclose their official role and position but make it clear that they do not necessarily speak on behalf of the school
- always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared
- always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws
- ensure that they have appropriate consent before sharing images on the official social media channel
- not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so
- not engage with any direct or private messaging with current pupils, parents/carers
- inform the DSL and Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils

12. How the school will respond to issues of misuse
Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and Internet acceptable use. The action taken will depend on

the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
All staff members will receive refresher training each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, bulletins and staff meetings).
By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety via MyConcern.
This policy will be reviewed every year by the DDSL. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

15. Links to other policies

- Child protection and Safeguarding Policy

- Behaviour
- Anti-bullying Policy
- Examinations
- Staff code of conduct
- Data protection policy

Appendix 1

SACRED HEART OF MARY GIRLS' SCHOOL

PUPILS' ACCEPTABLE USE AGREEMENT AGREEMENT

You must sign the School Internet Permission form to be granted access to the internet.
Agreement to the following will secure your online safety and ensure you are acting as a responsible digital citizen.

GENERAL USAGE

I will only use the school's computers for schoolwork, homework and as directed.
I will only transfer files to and from the school network using GoogleDrive.
I will only work on my own files on my own computer at all times.
I will keep my logins, IDs and passwords private at all times.
I will only log onto the school Network/ learning platform with my own username and password.
I will not download attachments or documents without the consent of my teacher.
I will report any issues with the school network to my teacher immediately.
I will not remove or tamper with ICT equipment and will report any damaged equipment to my teacher/network manager immediately.

EMAIL / COMMUNICATION

I will only use my school email address when using the school network/learning platform.
When communicating with staff/students I will be polite and respectful.
I am aware that all communications/activity is monitored across the school network at all times to protect and safeguard all members of the school community. This includes Google Classroom and any use of the Google Suite.

I will not give out any personal information such as phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
I acknowledge that emails sent outside of school hours will be treated as if they were sent on the morning of the next day the school is open.
The messages I send, or information I upload, will always be polite and sensible.
If I see anything I am unhappy with or I receive a message I do not like I will not respond to it, but I will save and talk to the teacher / trusted adult.

USE OF SOCIAL MEDIA

Pupils should be aware that content uploaded to social media is not private. Even if restricted to 'friends', there is still capacity for it to be re-posted or distributed beyond the intended recipients. Therefore, pupils using social media should conduct themselves politely and respectfully.
Pupils should not upload any content on to social media sites that:

- is confidential to the school or its staff
- amounts to bullying
- amounts to unlawful discrimination, harassment or victimisation
- brings the school into disrepute
- contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips
- undermines the reputation of the school and/or individuals
- is defamatory or knowingly false
- breaches copyright
- is in any other way unlawful.

USE OF INTERNET

I will be responsible for my own behaviour when using the internet.
I will not use work from the Internet as if it were my own. I will give credit to the sources of materials included in my work.
I will use the internet responsibly and will only visit websites approved by the school.
I will not attempt to bypass the internet filtering system.
I will not download software from the Internet
I am aware that, at all times, my online activity should not upset or hurt other people and I should not put myself at risk.
I am aware that my internet access can be restricted by the school should I fail to comply with the expectations outlined above.
I have read and understand these choices of behaviour are designed to keep me and our school community safe. I agree to them and understand that if they are not followed, school sanctions may be applied and my parent/carer may be contacted.

Appendix 2

SACRED HEART OF MARY GIRLS SCHOOL

ACCEPTABLE USE AGREEMENT AGREEMENT
STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

You must sign the School Internet Permission form to be granted access to the internet.
Agreement to the following will secure your online safety and ensure you are acting as a responsible digital citizen.

Staff should be aware that content uploaded to social media is not private. Even if restricted to 'friends', there is still capacity for it to be re-posted or distributed beyond the intended recipients. Therefore, staff using social media should conduct themselves with professionalism and respect.
Staff should not upload any content on to social media sites that:

- is confidential to the school or its staff
- amounts to bullying, unlawful discrimination, harassment or victimisation
- brings the school/trust into disrepute
- contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips
- undermines the reputation of the school and/or individuals
- is defamatory or knowingly false
- breaches copyright
- is in any other way unlawful.

Staff should note that the use of social media accounts during lesson time is not permitted.

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)

- Use them in any way which could harm the school's reputation
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Use my own devices to take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
I will only send work emails between the hours of 7.30am and 6.00pm
I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. Where possible I will use GoogleDrive.
I will let the designated safeguarding lead (DSL) and Network manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
SIGNED: DATE:

Appendix 3

Summary of where content is taught

Online Safety Across the School Audit

Appendix 4

Remote Learning

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

- During the period of remote learning, the school will maintain regular contact with parents to:
- Reinforce the importance of children staying safe online
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites
- Direct parents to useful resources to help them keep their children safe online

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.