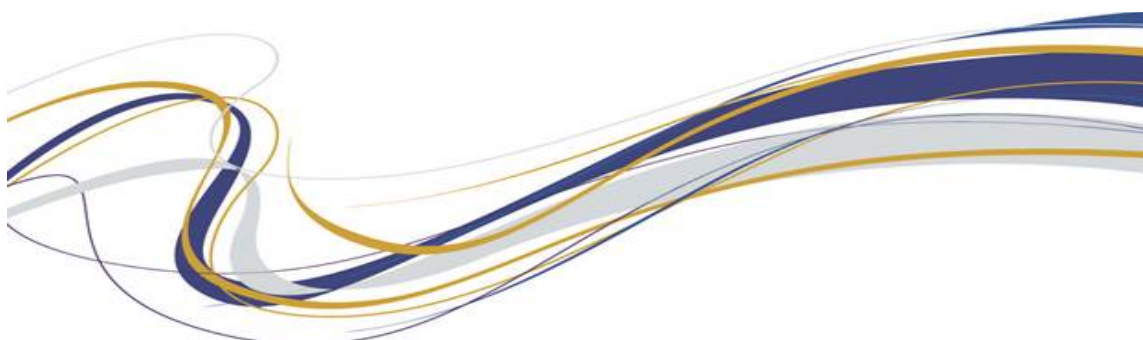# ONLINE SAFEGUARDING POLICY

**Committee responsible for review: Welfare Committee**

**Review date:  September 2021**

**Date of next review: September 2023**

<p align="center">__Online Safeguarding Policy__</p>

**We aim for All Hallows RC High School to be a Catholic school to which children wish to come, to which parents wish to send their children, and where teachers wish to teach.**

**Our Mission is to offer a high quality Catholic education for all, in an environment where Gospel Values are central to teaching and learning, and in which the unique value of each person is recognised and respected.**

**This policy runs alongside the School's Child Protection and Safeguarding Policy**

## Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

## Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

## Governors:

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

## Headteacher and Senior Leaders:

- The Headteacher and DSL are responsible for ensuring the safety (including Online Safety) of members of the school community
- The Headteacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

Online safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher and DSL ensures that the policy is implemented and compliance with the policy monitored. The responsibility for Online Safety has been designated to a member of the senior management team.

## Designated Safeguarding Lead

The Designated Safeguarding Lead (Mrs Done) is  trained in Online Safety issues and is aware of the potential for serious child Protection issues to arise from:

- sharing of personal data

- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

## RM On Site Technician

The onsite RM technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the Online Safety technical requirements outlined in any relevant Local Authority Online Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy

## Teaching and Support Staff

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures.  Central to this is fostering a 'no blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Teaching and support staff are also responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Online Safety Co-ordinator or senior leader for investigation, action and possible sanction

All staff should be familiar with the school's policy including:

- Safe use of e-mail
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs and use of website
- Online bullying procedures
- Their role in providing Online Safety/acceptable ICT use education for pupils
- Their role in preventing terrorism and extremism

Staff are reminded / updated about Online Safety matters at least once a year.

## Pupils

- are responsible for using the school ICT systems and mobile technologies in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

We include Online Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to minimise online risks and how to report a problem.  There is also a pupil friendly Online Safety policy to ensure pupil are aware of their responsibilities.

**Parents/Carers**

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local Online Safety campaigns and literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student/Pupil Acceptable Use Policy
- accessing the school ICT systems or Learning Platform in accordance with the school Acceptable Use Policy


**Online Safety Education and Training**


**Education – students / pupils**

Online Safety education will be provided in the following ways

- A planned Online Safety programme is provided as part of ICT lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information

Education & Training – Staff

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

- All staff will receive Online Safety training as part of their training programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies.


Communication devices and methods

The following table shows the school's policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

| Communication method or device | Staff & other adults | | | | Students/Pupils | | | |
|---|---|---|---|---|---|---|---|---|
| | Allowed | Allowed at break times | Allowed for selected | Not allowed | Allowed | Allowed at certain times | Allowed with staff | Not allowed |
| | ☑ | ⚠ | | ☒ | ☑ | ⚠ | ⚠ | ☒ |
| Mobile phones may be brought to school | ☑ | | | | | | | ☒ |
| Use of mobile phones in lessons | | | | ☒ | | | | ☒ |
| Use of mobile phones in social time | | ⚠ | | | | | | ☒ |
| Taking photos or videos on personal mobile phones or other camera devices | | | ⚠ | | | | | ☒ |
| Use of personal email addresses in school, or on school network | | ⚠ | | | | | | ☒ |
| Use of school email for personal emails | | | | ☒ | | | | ☒ |
| Use of chat rooms / facilities | | | | ☒ | | | | ☒ |
| Use of instant messaging | | | | ☒ | | | | ☒ |
| Use of social networking sites | | | | ☒ | | | | ☒ |

⚠ This table indicates when some of the methods or devices above may be allowed:

## Unsuitable/inappropriate 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:

| User Actions | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|
| **User Actions** | ☑ | ⚠ | ⚠ | ☒ | ☒ |
| 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 UK  Extremist or Terrorism related material | | | | | ☒ |
| Pornography | | | | | ☒ |
| promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability | | | | | ☒ |
| 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 SCC and / or 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 | | | | ☒ | |
| Accessing the internet for personal or social use (e.g. online shopping, banking etc) | | | | ☒ | |
| File sharing e.g. music, films etc | | | | ☒ | |
| Use of social networking sites | | | | ☒ | |
| Use of video broadcasting eg Youtube | | | | ☒ | |
| Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses) | | | | ☒ | |

Good practice guidelines

Email

Best practice →

☑ **DO**

Staff and students/pupils should only use their school email account to communicate with each other

Safe practice →

⚠

Check the school e-safety policy regarding use of your school email or the internet for personal use e.g. shopping

Poor practice →

☒ **DO NOT**

Staff: don't use your personal email account to communicate with students/pupils and their families without a manager's knowledge or permission – and in accordance with the e-safety policy.

## Images, photos and videos

**Best practice** →

☑ **DO**

Only use school equipment for taking pictures and videos.

Ensure parental permission is in place.

**Safe practice** →

⚠

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

**Poor practice** →

☒ **DO NOT**

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don't retain, copy or distribute images for your personal use.

Internet

**Best practice**

☑ **DO**

Understand how to search safely online and how to report inappropriate content .

**Safe practice**

⚠️

Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

**Poor practice**

☒ **DO NOT**

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

## Mobile phones

**Best practice** →

☑ **DO**

*Staff: If you need to use a mobile phone while on school business (trips etc), the school will should provide equipment for you.*

*Make sure you know about inbuilt software/ facilities and switch off if appropriate.*

**Safe practice** →

⚠

Check the e-safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first

**Poor practice** →

☒ **DO NOT**

Staff: Don't use your own phone without the Headteacher/SLT knowledge or permission.

Don't retain student/pupil/parental contact details for your personal use.

## Social networking (e.g. Facebook/ Twitter)

This guidance is to be applied outside of the school setting as social networking is not permitted in school. Schools should take into consideration the age of their pupils, and whether they are old enough to have accounts when sharing this guidance.

**Best practice** →

☑ **DO**

If you have a personal account, regularly check all settings and make sure your security settings are not open access.

Ask family and friends to not post tagged images of you on their open access profiles.

**Safe practice** →

⚠

Don't accept people you don't know as friends.

Be aware that belonging to a 'group' can allow access to your profile.

**Poor practice** →

☒ **DO NOT**

Don't have an open access profile that includes inappropriate personal information and images, photos or videos.

Staff:

Don't accept students/pupils or their parents as friends on your personal profile.

Don't accept ex-students/pupils users as friends.

Webcams

Best practice

☑ **DO**

Make sure you know about inbuilt software/
facilities and switch off when not in use.

Safe practice

⚠️

Check the e-safety policy for any instances
where using personal devices may be
allowed.

Always make sure you have the
Headteacher/SLT knowledge or permission

Make arrangements for pictures to be
downloaded to the school network
immediately after the event.

Poor practice

☒ **DO NOT**

Don't download images from organisation
equipment to your own equipment.

Don't use your own equipment without
Headteacher/SLT knowledge or permission –
and in accordance with the e-safety policy.

Don't retain, copy or distribute images for

**Sexting/Peer on Peer Abuse/Cyberbullying**

**All** staff should be aware that safeguarding issues can manifest themselves via peer on peer abuse. This could include cyberbullying and sexting (youth produced sexual imagery). Staff should be clear as to the school policy and procedures with regards to peer on peer abuse and sexual harassment.

Further guidance on Sexting and Cyberbullying and how to handle incidents can be found below:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

https://www.gov.uk/government/publications/preventing-and-tackling-bullying


**Searching devices, viewing and deleting imagery**

Adults should not view youth produced sexual imagery unless there is good and clear reason to do so.

If the capture involves Child Abuse images (or suspected child abuse images):

- Do not search of check a device for further images.  The device should be confiscated and further advice should be sought from the DSL.
- Do not print or copy images.
- Do not email a copy of the image to anybody.
- Do not show the image/capture to a minor.
- Do not show the image on the system to anybody who does not need to be exposed to the image.

***Any printing, emailing or copying of a child abuse image is an offence under English Law. A child abuse image or indecent image of a child is an image of a sexual nature which depicts a child under the age of 18.***

If the capture involves Adult pornography:

- Do not search of check a device for further images.  The device should be confiscated and further advice should be sought from the DSL.
- Do not print out or copy images out unless necessary
- Do not email a copy of the image to anybody, unless necessary
- Do not show the image on the system to anybody who does not need to be exposed to the image.
- Do not show the image/capture to a minor.

***An offence against English law may be committed if adult pornography image is shown to a child. If there is a need to print out the image to show an adult this must be kept secure and not for general circulation.***

**Filtering and Monitoring**

All Hallows will do all that they reasonably can to limit children's exposure to the risks below in regards to online material:

-content: being exposed to illegal, inappropriate or harmful material;

-contact: being subjected to harmful online interaction with other users; and

-conduct: personal online behaviour that increases the likelihood of, or causes, harm.

As part of this process the school has appropriate filters and monitoring systems in place. The appropriateness of these filters will be considered and governors and proprietors will consider a whole school approach to online safety.

Governors and proprietors will ensure that, staff to undergo regularly updated safeguarding training and that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

## Information and support

There is information available to support schools to keep children safe online. The following is not exhaustive:

www.thinkuknow.co.uk
www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.childnet.com/cyberbullying-guidance
www.pshe-association.org.uk
educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

## How Complaints will be handled

We will take all reasonable precautions to ensure Online Safety.  However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.  Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by teacher / PPL/ Child Protection Officer / DSL/ Headteacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework);
- Referral to LA / Police.

Our Designated Safeguarding Lead (Mrs Done) acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.


Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.  Complaints related to child protection are dealt with in accordance with the school's child protection procedures.