ONLINE SAFETY POLICY

2025-2026

Our Mission Statement

Our Lady of Grace RC Primary School recognises that each member of our community is unique and made in the image and likeness of God. Our School will encourage each member:

Through **WORK**, to develop his or her potential

Through **WORSHIP**, to learn to know and love God and His world

Through **WITNESS**, to proclaim to all the peace, joy and glory of God

As Catholics we live our faith through all aspects of our lives. Our Mission Statement underpins our thinking when implementing this procedure

Commitment to Equality:

We are committed to providing a positive working environment which is free from prejudice and unlawful discrimination and any form of harassment, bullying or victimisation. We have developed a number of key policies to ensure that the principles of Catholic Social Teaching in relation to human dignity and dignity in work become embedded into every aspect of school life and these policies are reviewed regularly in this regard.

1. INTRODUCTION

The purpose of this policy is to outline the safeguarding measures in place for all adults and children in Our Lady of Grace R.C. Primary School when using internet technologies and electronic communication.

Online Safety Lead:	**Miss J Skarratt**
Designated Safeguarding Lead:	**Mr T Collins**
Assistant Designated Safeguarding Lead:	**Mrs A Smith**
Safeguarding Governor:	**Mr M O'Doherty**
Chair of Governors:	**Mrs M Cunningham**

The Teacher Standards state that teachers, including Head teachers, should safeguard children's wellbeing and maintain public trust in the teaching profession as part of their professional duties. This agreement is available on the school website. Related documents include:

- Health & Safety & Premises Management Policy
- Safeguarding Policy
- Behaviour & Anti Bullying policies.
- The Staff Code of Conduct
- Whistleblowing Policy
- GDPR Policy

Consultation and/or Communication with the whole school community takes place regularly.

The Children's Online Safety (SMART) Rules can be found at the back of this document.

School uses DfE Approved SURF-PROTECT filtering and monitoring protection software.

2. RISKS

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information including voice/images.
- Inappropriate use of Artificial Intelligence Software (AI) Misinformation. Disinformation. Fake News. Conspiracy Theories
- Grooming by those with whom they make contact on the internet.
- The sharing of personal images without consent.
- Inappropriate communication including 'sexting'. (Peer to Peer)
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the accuracy of information on the internet.
- Copyright infringement.
- Illegal downloading/streaming of files
- The potential for excessive use impacting social and emotional development/learning.

Our Lady of Grace will endeavour to take all reasonable precautions to reduce all risks to children.

3. TEACHING AND LEARNING

- The Internet is an essential element for education, part of the statutory curriculum and a necessary tool.
- School Internet access is designed expressly for pupil use including appropriate content filtering.
- Pupils are given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils are educated in the effective use of the Internet in research, the skills of knowledge location, retrieval and evaluation.
- Children are monitored appropriately when using the internet.
- Our Computing Curriculum includes all key elements of staying safe online.
- Staff are aware of the need to comply with copyright law.
- All websites accessible from school have been assessed for suitability/potential harm.

4. GOVERNORS:

The Premises Committee/Full Governing Body regularly meet with the Designated Safeguarding Lead at school where the school's provision in relation to safeguarding (including Online Safety) is presented/reviewed. The Computing Lead presents to the Senior Leadership Team and/or Governors as part of their role.

5. ONLINE SAFETY LEADER AND SENIOR LEADERS

- Write and review the school Online Safety Policy
- Ensure that all staff/pupils are familiar with our Online Safety rules and procedures
- Provide staff and parents with advice/resources/training for teaching children about Online Safety
- Keep up-to-date with Online Safety issues and guidance through liaison with the Local Authority Schools' IT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP) and the Department For Education
- Ensure that all staff are aware of Safeguarding procedures to be followed in the event of an Online Safety incident taking place
- Facilitate the monitoring of the school's IT infrastructure is secure and is not open to misuse or malicious attack through weekly liaison with Holker & the monitoring security software
- Ensure that the network and internet access security requirements are in line with government legislation and any relevant Local Authority Online Safety Policy and guidance
- Ensure that users may only access the school's networks through a properly enforced password protection policy

6. TEACHING AND SUPPORT STAFF

- Have an up to date awareness of Online Safety matters and of the current school policy
- Are vigilant in their supervision of children accessing the internet
- Have read and understood our Online Safety policy
- Report any suspected misuse or problem to a Safeguarding Lead/Senior Leader for investigation/action

7. STUDENTS/PUPILS:

- Responsible for using the school IT systems & mobile technologies in line with the Online Safety rules
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

8. PARENTS/CARERS

- Support the School Online Safety Policy
- Reporting concerns/incidents

9. COMMUNITY USERS/THIRD PARTY

- Any users who access school IT systems as part of Extended School provision will be expected to follow school procedures for acceptable use of IT.

10. EDUCATION & TRAINING – STUDENTS / PUPILS

We embed Online Safety messages across the curriculum whenever relevant to the activity.

Online Safety education will be provided in the following ways:

- A planned Online Safety programme will be provided as part of IT and PHSE lessons and will be regularly revisited – this will cover both the use of IT and new technologies in and outside of school.
- Our curriculum will teach children about online harms relating to content, contact, conduct and commerce in an age-appropriate way
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities
- Online Safety rules will be posted around school.
- Students/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
- Key Online Safety messages are reinforced through assemblies and Internet Safety Day (February) and throughout lessons as appropriate.
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies.
- Staff members are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- In lessons where internet use is pre-planned, pupils are guided to sites suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Pupils are taught to be critically aware of the content they access on-line and are guided to validate the accuracy and reliability of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will agree to the Online Safety rules at the beginning of each year in KS1 and KS2.

11. EDUCATION & TRAINING – STAFF

- Online Safety training is made available to staff. Staff will have the opportunity to identify Online Safety as a training need within the appraisal process.
- All new staff will receive Online Safety information as part of their induction programme,

12. SOCIAL MEDIA POSTS & WEBSITE CONTENT STAFF

- Social Media Posts, photographs and videos are only to be taken/used to support learning experiences, promote the school, celebrate achievements and to provide useful information.
- The School Social Media accounts are only to be used by the Senior Leadership team in-line with guidance from the Headteacher, the Staff Code of Conduct, Teacher Standards & Safeguarding Policy.
- Images or videos that include pupils are to be selected carefully. Exclusion lists must be checked.
- Pupils' names are not to be used anywhere that could identify children by name.
- Permission from parents or carers will be obtained before images or videos of pupils are taken/shared.

13. INTERNET/SOCIAL MEDIA PUPILS

- Everyone is responsible for their own behaviour on the Internet.
- Pupils must ask permission before using the Internet & have a clear instruction on purpose.
- Children are only permitted to use Gmail addresses for email. All email will be monitored.
- Children will not engage in any form of conversation or dialogue with other users on the Internet without permission and supervision from staff, in which case communications will be closely monitored.
- The use of public chat rooms, internet messaging services and all social media platforms is prohibited.
- External/portable hard drives are prohibited.
- If any children are uncomfortable or upset by anything they discover on the Internet, they are taught to click on the Red Button and report it immediately to the supervising adult.
- Pupils in the Foundation Unit may log on using a year group login, but from Year 1 upwards, pupils should only access the network using their own personal login.

14. FILTERING AND MONITORING

All online activity is subject to filtering and monitoring systems. Harmful content is blocked and inappropriate activities are reported to both the Headteacher and the Online Safety Leader.

School uses SurfProtect, which fulfils the DfE's statutory filtering and monitoring requirements for schools and colleges.

SurfProtect is managed and maintained by our IT Support Company, Holker. Holker regularly liaise with the Online Safety Leader. This ensures all students are protected whilst still being able to access age appropriate content and that teaching and learning is not unreasonably impacted. The effectiveness of Surf Protect is reviewed by the Safeguarding Governor.

15. USE OF ARTIFICIAL INTELLIGENCE, MISINFORMATION, DISINFORMATION, FAKE NEWS, CONSPIRACY THEORIES

We recognise the valuable potential artificial intelligence (AI), including generative AI, holds for schools. These include customising learning experiences, preparing high quality resources quickly and supporting educational innovation/creativity.

We are aware of the risks posed by AI. These include data protection breaches, copyright issues, ethical complications, safeguarding and compliance with wider legal obligations.

STAFF

Whatever tools or resources are used to **support appropriate working practices** in school, the quality, safety and content of the final document/image/presentation/lesson aid etc. remains the professional responsibility of the person who produced it.

PUPILS

Currently, children at Our Lady of Grace do not have access to AI software. At home parents/carers are responsible for the safe/appropriate use of AI tools. Parents receive regular sign posting to support them with this through Newsletters and pages on the School Website.

School is committed to ensuring pupils develop the right skills to make the best use of AI as they move through the education system. The following topics are examples of content taught to the children which already supports future learning/use of AI:

- Creating and using digital content safely and responsibly.
- The limitations, reliability and potential bias of the Internet.
- How information on the internet is organised and ranked.
- Online safety lessons to protect themselves against harmful or misleading content.

16. PUBLISHED CONTENT AND THE SCHOOL WEBSITE

- The website is regularly monitored to ensure that there is no content that compromises the safety of pupils or staff.
- School maintains and adheres to up to date 'Exclusion Lists' (not consented/safeguarding concern).
- Staff and pupils' personal information is never published.
- The school website does not publish content which can connect a child's image with their name.
- Image/document files are appropriately named for use online.

17. PERSONAL MOBILE DEVICES (INCLUDING PHONES)

- The school allows staff to bring in personal mobile phones and devices for use during non-contact time.
- Only under exceptional circumstances should a member of staff contact a parent/carer using their personal device. On these occasions, the member of staff should dial '141' before the phone number to prevent parents from identifying their personal phone number.
- The school does not allow pupils to bring personal mobile devices into school unless previously agreed. Any device must be handed to the class teacher at the beginning of the day to be stored safely.
- Permission must be sought before any image or sound recordings are made of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

18. MANAGING EMERGING TECHNOLOGIES

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

19. RESOURCES

All school resources are protected by the school alarm system. School has an asset management software package which is updated annually.

Pupils are taught to handle the IT resources appropriately with care to prevent any damage and are instructed to report any damage or breakdown of equipment immediately to the adult in charge.

All software in school is correctly licensed either by multiple single licenses or site licenses. No user is permitted upload software onto the computers unless the Headteacher has authorised them to do so.

20. INCIDENT MANAGEMENT

It is important that any incidents are logged then dealt with quickly and proportionate to the offence. The school will decide what constitutes inappropriate use and the sanctions to be applied.

- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaint's procedure.
- CPOMS should be updated where appropriate (see Safeguarding Policy).,

21. DATA PROTECTION AND PRIVACY

At Our Lady of Grace R.C. Primary School we ensure that all of our stored data is protected from unauthorised access. The children's personal records as well as staff information are protected and only access through authorised personnel. The information is protected via a password and access through a server which is maintained and backed up by Holker IT.

Staff must use their own secure G-Drive if moving private/confidential information between sites.

The school allows these members of the school community (pupils, teachers and assistants) to store data on the school's IT resources (for example school network etc.). This network is protected via a password and access is monitored. We do not allow any transfer of data to the school system from external sources unless approved by Holker IT.

The school collects information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school. We ensure that all personal information supplied is held securely in accordance with the policies and practices as defined by the Data Protection Act.

KEY STAGE 1

Our Online Safety Rules

1) I will only use the internet when my **teacher** is with me.
2) I will only visit websites that my **teacher allows me to**.
3) I will only send **polite and friendly messages** to others.
4) I will never let other people know my **personal information**.
5) I will click on the **Red Button** then tell my teacher straight away if I see anything that is **not nice** on the internet.

6) I will only click on buttons when **I know what they do.**
7) I will always follow the **SMART Rules!**

KEY STAGE 2

Our Online Safety Rules

1) I must always **ask for permission** before I use the internet.
2) I can only visit the websites that my teacher **has allowed me to**.
3) I must click on the **Red Button** then **tell my teacher straight away** if I see something that is inappropriate.

4) I must **tell a teacher straight away if I** see anyone else using the internet inappropriately.
5) I must never give anyone any **personal details about myself** online.
6) I must **always** keep my **passwords private**.
7) I must **always** be **polite and respectful** online.
8) I am **not allowed** to use Social Media websites.
9) I will **always** follow the **SMART Rules!**