E-SAFETY AGREEMENT

2024

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

The purpose of this agreement 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. It describes:

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 and supports the school Behaviour, Health & Safety, Safeguarding and Anti Bullying policies.

Consultation with the whole school community has taken place through:

Forum	Date
Staff meeting	***March 2023***
Pupil Assembly	***March 2024***
Governors' meeting	***June 2024***
Parents' meeting	***March 2023***
School website / newsletters	***March 2024***

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

School uses SMOOTHWALL filtering and monitoring protection software.

Risks

Our Lady of Grace we are aware of the serious risks involved and the need to safeguard our pupils from the dangers that they may face online.

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- 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 which may impact on the social and emotional development and learning of the young person.

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

Teaching and Learning

- The Internet is an essential element for education. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The 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 will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Children will be monitored appropriately when using the internet.
- As part of the new Computing Curriculum, we will focus on different elements of staying safe on line.
- The school will make staff and pupils aware of the need to comply with copyright law.
- When children are directed to websites as part of home learning they will have been checked for appropriateness.

Governors:

The Premises Committee regularly meet with the Designated Safeguarding Lead at school (Mr T Collins) where the school's provision in relation to safeguarding is presented. Miss Skarratt the Computing Lead also presents to the Senior Leadership Team and/or Governors as part of her role.

E-Safety Leader and Senior Leaders

- has a leading role in establishing and reviewing the school E-Safety policy
- ensures that all staff are provided with our E-Safety rules and procedures
- provides staff with advice/resources for teaching their children about E-Safety
- keeps up-to-date with E-Safety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).

- 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 or arranges training and advice for staff and parents
- ensures that the school's ICT infrastructure is secure and is not open to misuse or malicious attack through weekly monitoring and updates of Sophos Security software
- ensures that the network and internet access security requirements are in line with government legislation and any relevant Local Authority E-Safety Policy and guidance
- ensures that users may only access the school's networks through a properly enforced password protection policy

Teaching and Support Staff

- they have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
- are vigilant in their supervision of children accessing the internet
- they have read and understood our E-Safety policy
- they report any suspected misuse or problem to a senior leader for investigation/action/sanction

Students/pupils:

- are responsible for using the school ICT systems and mobile technologies in accordance with the e-safety rules
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents/Carers

- supporting the school e-safety policy
- reporting concerns/incidents

Community Users

Community Users who access school ICT systems as part of the Extended School provision will be expected to follow school procedures for acceptable use of ICT.

E-Safety Education and Training

Education – students / pupils

We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used.

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

- The E-Safety policy will be introduced to the pupils at the start of each school year
- A planned E-Safety programme will be provided as part of ICT and PHSE lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside of school
- Key E-Safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities
- E-Safety rules will be posted in all networked rooms.
- 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 E-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 checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches. Staff pre-check any 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 e-safety rules at the beginning of each year in KS1 and KS2.**

Education & Training – Staff

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

- A planned programme of formal E-Safety training will be made available to staff. Staff will identify E-Safety as a training need within the approval process including the receipt of a Staff Handbook and Code of Conduct.
- All new staff will receive E-Safety information as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable Use Policies.

Use of digital and video images

Photographs and video taken within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's website and to provide information about the school on the website. The school will:

- When using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.

- Allow staff to take images to support educational aims, but follow guidance concerning the sharing, distribution and publication of those images.

- Make sure that images or videos that include pupils will be selected carefully and will not provide material that could be reused.

- Make sure that pupils' names will not be used anywhere on the school website in association with photographs.

- Written permission from parents or carers will be obtained before images or videos of pupils are electronically published.

- Keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use.

Internet

- We expect everyone to be responsible for their own behaviour on the Internet, just as they are anywhere else in school.
- Pupils must always ask permission before using the Internet and have a clear idea why they are using it.
- Children are only permitted to use G Mail addresses for email. All email will be moderated and monitored by the class teacher. The use of unfiltered web-based email is not permitted.
- Children will not engage in any form of conversation or dialogue with other users on the Internet without permission and supervision from their teacher, in which case communications will be monitored.
- The use of public chat rooms and Internet Messaging Services is prohibited.
- The use of social networking sites such as e.g., Facebook are not permitted. These cannot be accessed in school as they are blocked by the Local Authority firewall.
- Computers should only be used for schoolwork and homework.
- Files may only be downloaded by staff, or children under supervision.
- Pupils using the Internet are expected not to deliberately seek out offensive materials. Should any such material be encountered accidentally, or if any children are uncomfortable or upset by anything they discover on the Internet, they will click on Hector immediately and report it immediately to the supervising adult. (Any adult should report it to the Designated Safeguarding Lead. Arrangements can then be made to request that the ISP blocks the site).
- Pupils in the Foundation Unit may log on using a year group login, but from Year 1 upwards, pupils should generally only access the network using their own personal login. No network user should access other people's files unless permission has been given.
- Any infringement of these conditions of use will be dealt with by the class teacher/Head Teacher as appropriate and sanctions may apply. Parents will be informed.

Published Content and the School Website

- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- Staff and pupils' personal information will not be published.
- The publications of children's work will be decided by a teacher.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Photographs and video focusing on individual children will not be published on the school website without parental permission.
- The school website will avoid publishing the full names of individuals in a photograph.
- The school will ensure that the image files are appropriately named and will not use pupils' names in image file names if published on the web.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Only under exceptional circumstances should a member of staff contact a pupil or parent/carer using their personal device. The school has a 'school mobile' which should be used where possible.
- 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. A log will be completed by the teacher.
- 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.

Digital/Video Cameras

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the guidelines set out in this document under 'Published Content'.
- Parents will not use digital cameras, mobile phones or video equipment at school unless specifically authorised by staff.

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.

Resources

The storage of ICT resources is of paramount importance. All classroom based computer systems are protected by the school alarm system.

Pupils are taught to handle the ICT 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. We do not allow any member of the school community to load software onto the computers unless the ICT co-ordinator has checked the copyright.

Incident Management – Pupils

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 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 complaints procedure.

Incident Management – Staff

Please refer to the Whistleblowing procedure

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 modem that is monitored. Physical integrity is maintained by performing backups to secure media on a set timetable.

Staff must use a date encrypted USB Memory Stick if storing any private/confidential information. These can be obtained from the IT Leader who will log the lending of the item.

The school allows these members of the school community (pupils, teachers and assistants) to store data on the schools ICT resources (for example school network etc.). This network is protected via a password and has access only during school hours. We do not allow any transfer of data to the school system from outside unless it comes through our filtered system.

The school collects information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school. The school will hold personal information on its systems for as long as the pupil remains a member of the school community and will remove it in the event of them leaving or until it is no longer required for the legitimate function of the school. We ensure that all personal information supplied is held securely in accordance with the policies and practices of Bury LA and as defined by the Data Protection Act 1998.

Introducing the E-Safety policy to pupils

Appropriate elements of the E-Safety policy will be shared with pupils at the start of the school year and revisited on a regular basis.

E-Safety rules will be posted in all networked rooms.

Pupils will be informed that network and Internet use will be monitored.

Curriculum opportunities to gain awareness of E-Safety issues and how best to deal with them will be provided for pupils.

Staff and the E-Safety policy

All staff will be given the School E-Safety Policy and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user.

Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

Parents'/guardians' attention will be drawn to the School E-Safety Policy in newsletters and on the school web site.

Parents and carers will from time to time be provided with additional information on E-Safety.

The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Please do not hesitate to arrange an appointment with Miss Skarratt if you require more information on or clarification of any aspect of this agreement.

Reviewed 2024

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the head teacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. If appropriate I will use a data encrypted memory stick.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to a member of the Senior Leadership team or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

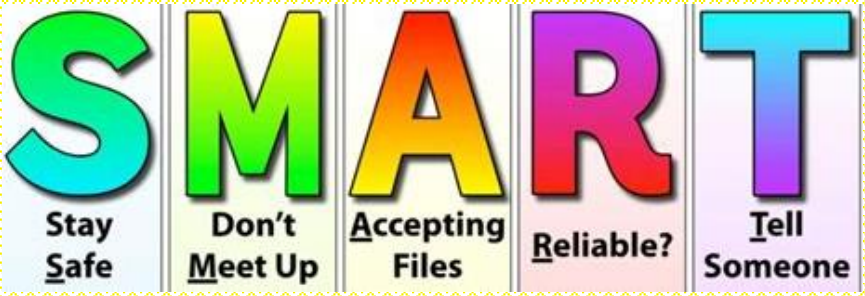
All staff have read, understood and agree with the Information Systems Code of Conduct.

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!**