St Gregory's
CATHOLIC PRIMARY SCHOOL

Pursuing Excellence:
Welcoming All

# St Gregory’s Catholic Primary School

## E-Safety and Acceptable Use Policy

| | |
|---|---|
| **Members of staff responsible:** | **Mr. John Daley** |
| **Date policy approved by the Governors:** | **January 2018** |
| **Date to be reviewed:** | **Autumn term 2021** |

**Our Mission Statement**

**“At the heart of our community, our mission is to treat others the way that we would like to be treated, to provide a caring and stimulating environment whilst promoting enthusiasm for life-long learning where all individuals feel respected, challenged and inspired to achieve their full potential.**
**A school of the future, growing and working together in God’s family and realising the champion within.”**

### ***Writing and Reviewing the E-Safety Policy***

- The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, behaviour and for child protection.
- The school’s E-Safety Coordinator is the Designated Child Protection Person as the roles overlap.
  It is not a technical role.
- Our E-Safety Policy has been written by the school. It has been agreed by all staff and approved by Governors.

### ***Teaching and Learning***

**Internet Access**

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

- □Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- □Internet use will enhance learning
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not, and be given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- □Pupils will be shown how to publish and present information to a wider audience.
- Pupils will be taught how to evaluate Internet content.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- □Pupils will be taught the importance of cross-checking information, before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

### E-mail

- When available, pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mails.
- In e-mail or on the web pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mails from pupils to external bodies are presented and controlled.
- The forwarding of chain letters is not permitted.

### Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- □Photographs that include pupils will be selected carefully ensuring parents have given their permission.
- Pupils' names will not be used in association with photographs anywhere on the school Website or other on-line space.
- □Pictures and work will only be shown on the website if parents/carers have signed the consent form issued when the child starts school.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

### Social networking and personal publishing

- □If they are to be used, the school will control access to social networking sites, and consider how to educate pupils in their safe use
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- □Pupils will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- □Pupils will be advised to use nicknames and avatars when using social networking sites.

### 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.
- Teachers are to be aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones will be kept under review.
- Games machines including the Sony Playstation, Microsoft Xbox and others which have Internet access may not include filtering. These may not be used in school.

***Protecting personal data***

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

***Procedures***

- The School ICT system's security will be reviewed regularly.

- Virus protection will be updated regularly.

- An acceptable use posters will be displayed adjacent to all classroom workstations and next to the laptop trolley.

- The school will work in partnership with parents, the LA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator and the School Network Manager and the E-Safety Coordinator informed.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

- E-Safety training will be embedded within the ICT scheme of work.

- E-Safety briefings and materials will regularly be made available to parents.

- Staff will always use a suitable and safe search engine when accessing the web with pupils.

- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family e.g. (but not limited to) SMS text message, email, instant messaging or telephone. Should special circumstances arise where such communication is felt to be necessary, the agreement of the headteacher should be sought first and appropriate professional language should always be used.

□□ Staff must not use mobile phones during teaching time or use camera phones.

***Handling e-safety complaints***

- Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the headteacher.
- 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 (see schools complaints policy).
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

***Enlisting parents' and carers' support***

- Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters and on the school website.
- The school will ask all parents to sign the parent /pupil agreement at the start of each school year or when children are admitted in the case of in-year admissions.

# St Gregory’s Catholic Primary School
# E-Safety and Acceptable Use Policy

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

□ I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

□ I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
.

□ I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.

□ I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.

□ I will not install any software or hardware without permission.

□ I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises.

□ I will respect copyright.

□ I will report any incidents of concern regarding children’s safety to the e-Safety Coordinator.

□ I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school’s information systems and Internet access, to intercept e-mail and to delete 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.

Signed: ……………………………… Capitals: ……………………… Date: ………