# Christ the King Catholic Primary School

## *E-safety Policy*

| Date | Review date | Coordinator |
|---|---|---|
| October 2021 | October 2022 | Mrs Rachael Kennedy |

***Our Vision: To provide an outstanding Catholic education with Christ as our light and our guide.***

Internet technology helps pupils learn creatively and effectively. It encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The e-safety policy encourages appropriate and safe conduct and behaviour during this process.

Pupils, staff and all other users of school-related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour.

These agreements and their implementation will promote positive behaviour at school. This can transfer directly into each pupil's adult life and prepare them for experiences and expectations in the workplace. The policy is not designed to be a blacklist of prohibited activities; it is a list of areas to discuss, teach and inform. It will develop positive behaviour and knowledge leading to safer internet use and year-on-year improvement, with a measurable impact on e-safety. The positive effects of the policy are intended to be seen online and offline in school and at home, and ultimately beyond school and into the workplace.

**The e-safety policy covers the use of**

- Mobile phones when used on the school site
- Pupils' and staff's personal ICT equipment when used in school and which makes use of school networking, file-serving or internet facilities
- External access to internal school networking such as webmail, network access, file-serving (document folders) and printing
- School-related external internet including, but not limited to, extranet, e-learning platforms, blogs, social media websites
- School-based intranet and networking
- School-based ICT systems and equipment

**Reviewing and evaluating e-safety and ensuring good practice – introduction**

E-safety policy results from a continuous cycle of evaluation and review based on new initiatives and partnership discussion with stakeholders and outside organisations, technological and internet developments, current Government guidance and school-related e-safety incidents. The policy development cycle develops good practice within the teaching curriculum and wider pastoral curriculum. Regular assessment of strengths and weaknesses helps to determine inset provision for staff and governors and guidance for parents, pupils and local partnerships.

The e-safety committee will actively monitor and evaluate the e-safety policy. This committee will comprise:

- Child protection officers Mr Mark Ryan and Miss Helen Lickess
- Pupils, e.g. a member of the School Council and our Digital Leaders
- Community stakeholders, e.g. nurseries, youth groups, sports clubs, faith groups/representatives
- Parents and guardians, e.g. PTA, parent governors, looked-after children/social care representatives
- Governor(s) ICT Governor

- ICT technical support and network manager
- In the event of an e-safety incident, the following people will be informed within school and in external agencies and stakeholder organisations. coordinator: Mrs Rachael Kennedy; Safeguarding officers: Mr Mark Ryan and Miss Helen Lickess
- Teaching staff
- Head teacher and school leadership team
- E-safety co-ordinator/officer Mrs Rachael Kennedy

When will your e-safety policy and acceptable use policies be reviewed?

- At or prior to the start of each academic year

Additionally, the policy will be reviewed promptly upon:

- Advice from the police
- E-safety incidents in the community or local schools which might impact on the school community
- Significant changes in technology as used by the school or pupils in the wider community
- New guidance by Government/LEA/safeguarding authorities
- Serious and/or frequent breaches of the acceptable internet use policy or other in the light of e-safety incidents

Where will the e-safety policy review be documented?

- In the school development plan

The school will draw up an e-safety calendar detailing training, meetings, reviews, evaluations, teaching and learning provision, parental involvement, wider community involvement and governor involvement over an academic year.

Staff, parent and pupil e-safety audits and pupil questionnaires will inform e-safety learning and staff training requirements. This will gauge the impact and effectiveness of the e-safety provision and determine future e-safety targets.

**Policy review schedule**

The e-safety committee and e-safety co-ordinator/officer will include evidence of evaluations of the impact of the e-safety policy in reports. Such evidence includes:

- E-safety audits of staff, support staff, parents, governors and other stakeholders
- AfL teaching questionnaires
- Reports to Governors

The governing body/proprietor will receive a report on the progress, evaluation, impact and effectiveness of the e-safety policy annually. This report will include suitably redacted e-safety incident accounts and statistics, detailing how they have been resolved, and the counter measures that were implemented.

**Who does e-safety affect? Who is responsible for e-safety and what are their roles?**

**School management and e-safety**

School senior management is responsible for determining, evaluating and reviewing e-safety policies. This encompasses teaching and learning, use of school IT equipment and facilities by pupils, staff and visitors. It also includes agreed criteria for acceptable use by pupils, school staff and governors of internet-capable equipment for school-related purposes or in situations which will impact on the reputation of the school, and/or on school premises.

E-safety provision is always designed to encourage positive behaviours and practical real-world strategies for all members of the school and wider school community.

Evidence base:

- Staff inset provision audit and record
- Regularly updated e-safety policy, child protection policy and logged and evaluated e-safety incidents
- Minutes from e-safety-related meetings with staff, SLT, parents association, governors and wider school community stakeholders
- E-safety calendar
- School development plan

**The school e-safety officer or co-ordinator**

The school's designated e-safety officer Mrs Rachael Kennedy reports to the SLT and governors and co-ordinates e-safety provision across the school and wider school community. The committee liaises with SLT, the school's designated child protection officer and other senior managers as required.

The school e-safety officer has a specific job description and person specification detailing the role, remit, qualifications and qualities required for the post. This specification is updated according to the school cycle for reviewing job descriptions.

**E-safety co-ordinator job description**

- The e-safety co-ordinator is responsible for promoting best practice in e-safety within the wider school community, including providing and being a source of information for parents and partner stakeholders.
- Although all staff are responsible for upholding the school e-safety policy and implementing safer internet practice, Mrs Rachael Kennedy is responsible for monitoring internet use by pupils and staff onsite, and on school machines such as laptops used off-site.
- The school e-safety co-ordinator audits and assesses inset requirements for staff, support staff and governor e-safety training, ensuring that all staff are aware of their responsibilities and the school's e-safety procedures. The co-ordinator is the first port of call for staff requiring advice on e-safety matters.

The school's e-safety co-ordinator chairs the school e-safety committee which includes representatives of the school SLT, teaching and support staff, governors, parents, pupils and the wider school community including relevant local stakeholders.

The co-ordinator:

- Is responsible for monitoring, reporting and evaluating incidences of inappropriate internet use.
- Is the first point of contact in an e-safety incident and is responsible for monitoring and reviewing e-safety incident logs.
- Is responsible for acting as a point of contact for support and advice on e-safety issues.
- Is responsible for promoting e-safety awareness for parents and wider stakeholders.
- Is responsible for ensuring e-safety is embedded in the curriculum, e.g. in schemes of work, assemblies and themed weeks.
- Is responsible for ensuring staff receive information about current trends.
- Is responsible for managing e-safety training for all staff.
- Is responsible for ensuring acceptable use policies/school internet rules are in place, agreed by staff, pupils and parents and are monitored, evaluated and reviewed.
- Is responsible for ensuring the e-safety policy is adhered to.
- Is responsible for ensuring that the e-safety policy links with other appropriate school policies, e.g. anti-bullying, child protection, Computing, PSHE.
- Is responsible for evaluating and reviewing the school's e-safety policy, updating at least annually.
- Is responsible for promoting a school and community-wide e-safety culture and promoting the school's e-safety vision to all stakeholders.
- Is responsible for completing regular e-safety audits and maintaining the e-safety calendar in conjunction with the senior leadership team and/or headteacher.

**Person specification and training requirement for e-safety officer/co-ordinator**

The school e-safety officer/co-ordinator will undertake relevant training where appropriate.

**Governors' responsibility for e-safety**

All e-safety and safe-guarding issues are adhered to.

**ICT support staff and external contractors**

At least one governor is responsible for e-safety. The school e-safety officer/co-ordinator will liaise directly with the governor about reports on e-safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community.

The e-safety officer/co-ordinator will be responsible for auditing governor e-safety training and inset requirements.

**Teaching and teaching support staff**

Teaching and teaching support staff ensure that they are aware of the current school e-safety policy, practices and associated procedures for reporting e-safety incidents.

All staff must ensure that they have read, understood and signed (thereby indicating an agreement) the acceptable use policies relevant to internet and computer use in school.

All staff must follow the school's social media policy regarding external off-site use, personal use (being mindful of bringing the school into disrepute), possible contractual obligations, and conduct on internet school messaging or communication platforms, e.g. email, VLE messages and forums and the school website.

All teaching staff must rigorously monitor pupil internet and computer use in line with the policy. This includes the use of personal technology such as cameras, phones and other gadgets on the school site.

Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.

Internet use and suggested websites should be pre-vetted and documented in lesson planning.

**Child protection officer**

The Child Protection Officer is able to differentiate which e-safety incidents are required to be reported to CEOP, local police, LADO, social services and parents/guardians. The individual will also determine whether the information from such an incident should be restricted to nominated members of the leadership team.

The child protection officer knows how to deal appropriately with incidents including (but not limited to):

- Allegations against members of staff
- Computer crime, e.g. hacking of school systems
- Allegations or evidence of 'grooming'
- Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.

The Child Protection Officer is responsible for acting 'in loco parentis' and liaising with websites and social media platforms such as Twitter and Facebook to remove instances of illegal material or cyber-bullying.

**Pupils**

Pupils are required to use school internet and computer systems in agreement with the terms specified in the school's acceptable use policies. Pupils are expected to sign the policy to indicate agreement, and/or have their parents/guardians sign on their behalf.

Pupils are aware of how to report e-safety incidents in school, and how to use external reporting facilities, such as the CEOP report abuse button.

Pupils are aware that their internet use out of school on social networking sites such as Facebook is covered under the acceptable use policy if it impacts on the school and/or its staff and pupils in terms of cyber-bullying, reputation or illegal activities.

**Parents and guardians**

It is hoped that parents and guardians will support the school's stance on promoting good internet behaviour and responsible use of IT equipment both at school and at home.

The school expects parents and guardians to sign the school's acceptable use polices, indicating agreement regarding their child's use and also their own use with regard to parental access to school systems such as extranets, websites, forums, social media, online reporting arrangements, questionnaires and the VLE.

**Parents**

The school will provide opportunities to educate parents with regard to e-safety, including:

- Twilight courses or a series of presentations run by the school for parents and wider school community stakeholders.
- Parents' evenings, open days, transition evenings, or other events to take advantage of occasions when there are large numbers of parents in school.
- E-safety information delivered to parents directly, including: letters, newsletters, website-subscribed news emails (accessed from *e-safetysupport.com*), the school extranet, learning platform, website or VLE.

**Guidance for other users**

Other users such as school visitors, wider school community stakeholders or external contractors are expected to agree to a visitor's AUP document or a tailored AUP document specific to their level of access and usage.

External users with significant access to school systems including sensitive information or information held securely under the Data Protection Act should be CRB-checked. This includes external contractors who might maintain the school domain name and web hosting, which would facilitate access to cloud file storage, website documents and email.

**How does the school provide e-safety education?**

Possible curriculum opportunities:

- E-safety events, e.g. Safer Internet Day and Anti-Bullying Week.
- E-safety as part of pastoral care including: assemblies; year group presentations; tutorial opportunities.
- E-safety as an ICT/computing teaching unit including (but not limited to): how to judge the validity of website information; how to remove cyber-bullying; computer usage and the law; how to spot and remove viruses; why copyright is important.

**Wider school community and stakeholders**

Possible information dissemination opportunities:

- Twilight courses or a series of presentations run by the school for parents and wider school community stakeholders.
- Open days or other events to take advantage of occasions when there are large numbers of visitors in school.
- E-safety information delivered to stakeholder directly, including: letters; newsletters; website-subscribed news emails; school extranet; learning platform; website; or VLE.

**Staff – inset and training**

E-safety information directly delivered to staff including: letters; newsletters; website-subscribed news emails; school extranet; learning platform; website; or VLE.

This provision will be evidenced in the following school documents:

- The school's CPD policy as well as the Headteacher's Professional Development Records.

A planned calendar programme of e-safety training opportunities to be made available for staff including: on-site inset; whole staff training; online training opportunities (for example NAACE courses); external CPD courses; accredited CPD courses (for example cyber-mentors or CEOP); and co-ordinator training.

This provision will be evidenced in the following school documents:

The e-safety policy will be updated and evaluated by staff at the beginning of each academic year and timetabled into the INSET day schedule.

The e-safety co-ordinator/officer should be the first port of call for staff requiring e-safety advice.

**Governors – training**

Possible training and information dissemination opportunities:

- Governors should also be given access to staff inset training and to specific governor training provided externally (for example by the LEA, NAACE online or the National Governors Association).
- Twilight courses or a series of presentations run by the school for parents and wider school community stakeholders.
- Open days or other events to take advantage of occasions when there are large numbers of visitors in school.
- E-safety information delivered to governors directly including: letters; newsletters; website-subscribed news emails (E-safety support.com); school extranet; learning platform; website; or VLE.
- Annual Governor's Review Day.

| | | | |
|---|---|---|---|
| **Headteacher:** | Mark Ryan | **Date:** | October 2021 |
| **Chair of Governing Body:** | | **Date:** | |