Crofton Junior School

E-Safety Policy

December 2017

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.

E-safety policy scope

The school e-safety policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider school community who use, have access to, or maintain school and school-related internet and computer systems internally and externally.

The school will make reasonable use of relevant legislation and guidelines to effect positive behaviour regarding ICT and internet use on and off the school site. This will include imposing rewards and sanctions for behaviour and penalties for inappropriate behaviour as defined as 'regulation of student behaviour' under the Education and Inspections Act 2006. 'In loco parentis' provision under the Children Act 1989 allows the school to report and act on instances of cyber-bullying, abuse, harassment, malicious communication and grossly offensive material. This includes reporting to the police, social media websites, and hosting providers on behalf of pupils.

The e-safety policy covers the use of

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

Reviewing and evaluating e-safety and ensuring good practice

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.

This policy will be reviewed every year in line with the school's policy review programme. The Head teacher is responsible for reporting to the Governors' about the quality of its implementation and its impact on standards. In the light of this, policy amendments may be made.
The e-safety committee will actively monitor and evaluate the e-safety policy. This committee will comprise:

- Head teacher and school leadership team
- Teaching staff
- ICT technical support and network manager
- Governor(s)

The policy will be reviewed promptly upon:

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

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.

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.

Management is encouraged to be aspirational and innovative in developing strategies for e-safety provision, which will deliver measurable success via a calendar of e-safety provision. Management should clearly state e-safety targets with success criteria on the school development plan.

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.

Teaching and teaching support staff will be provided with an e-safety induction as part of the overall staff induction procedures.

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.

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 school acceptable use policies cover all computer, internet and gadget usage in school, including the use of personal items such as phones.

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:

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

How does the school provide e-safety education?

Possible curriculum 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.
- E-safety as a PSHE teaching unit including (but not limited to): how to deal with cyber-bullying; how to report cyber-bullying; the social effects of spending too much time online.

- E-safety as part of pastoral care including: form time activities; assemblies; year group presentations; tutorial opportunities.
- E-safety events, e.g. Safer Internet Day and Anti-Bullying Week.

Wider school community and stakeholders

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.

Governors – training

Possible training and information dissemination opportunities:

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

The policy is reviewed every 12 months, in consultation with the whole school community including staff, pupils, parents, carers and governors.

Date of last review: 6th December 2017
Head teacher signed: P. Birdsall
Chair of Governors signed: J. Allen