Croft Primary School

Internet Safety

Context

The internet has undoubtedly become an integral part of our lives. Many people use the internet or internet services to perform daily tasks and it has certainly become an essential element in our ever-expanding technological age. We must recognise that the internet and its applications hugely impact upon all aspects of our life including school, business and social interactions. The internet is widely used in school by all staff and by children during taught sessions. It is the duty and responsibility of **all staff** to ensure that pupils are using the internet safely and responsibly in school and that they understand the importance of online safety and how it can be applied to situations outside of school.

The Computing Subject Leader (Mr Bonser) has the responsibility for ensuring that all staff are aware of our Online Safety Policy and receive regular updates on its content.

Scope of the policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both inside and outside of school.

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other online safety incidents covered by this policy, which may take place outside of Croft Primary School, but is linked to membership of the Croft Primary School. The 2011 Education Act increased these powers with regards to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by our current behaviour policy.

The school will deal with such incidents within this policy (and the associated Behaviour and Anti-Bullying policies) and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Aim of the policy

The aim of this policy is to ensure that pupils are equipped with knowledge and skills when working within the Croft Primary School's managed environment and away from it. It is important that pupils are given opportunities to learn how to assess and manage potential risks for themselves. It is equally important that staff have access to regular Online Safety training and are informed of any current thinking or changes in practice. We also have a duty of care to our parents and offer Online Safety updates via newsletters and information on the school website.

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

DRAFT

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Relationships education and health education in primary schools

Searching, screening and confiscation

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
The policy also takes into account the National Curriculum computing programmes of study.

DRAFT

Roles and responsibilities

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

Head Teacher:

The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Computing Lead.

The Head Teacher (Designated Safeguarding Lead) and other designated safeguarding members of staff are ensuring that any online safety incidents and or cyber bullying incidents are logged and dealt with appropriately in line with this policy and the behaviour policy. They are also aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

Computing Lead:

Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school policies for computing and online safety.

- 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 training and advice for staff.
- Liaises with school technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future online safety developments.

Technical staff: Technical staff in contract to support school with ICT and computing are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.

- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That they keep up to date with online safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head Teacher/Computing Lead for investigation / action / sanction.
- The school ICT system security is reviewed regularly. Virus protection is updated regularly.

Managing filtering

- The school will work with the LGFL School Potect and our IT technicians to ensure systems to protect staff and pupils are effective and reviewed regularly.
- Any unsuitable on-line material should be reported to the Computing Lead and DSL.
- Regular checks will be made to ensure the filtering methods are appropriate, effective and reasonable.
- A log will be kept and used to identify patterns and behaviours and therefore inform policy and educational interventions.
  Routine Monitoring will be established once it is available via LGFL. Sensio software.

Teaching and Support Staff:

All teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices and implement them consistently.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP).
- They report any suspected misuse or problem to the Head Teacher/Computing Lead for investigation, action or sanction.
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using the agreed school procedure.
- Online safety awareness is embedded in all aspects of the curriculum and other activities and is regularly revisited.
- Pupils understand and follow the online safety and acceptable use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, including, but not limited to laptops, chromebooks i-pads and cameras in lessons and other school activities where allowed and implement current policies with regards to these devices.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils:

All pupils are aware of the course of action should they come across something worrying, a pop up or communication from an unknown source. are responsible for using the school digital technology systems safely; have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations; need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

All pupils should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Croft Primary School's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers:

DRAFT

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Croft Primary School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, our website and information about e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website.
- their children's personal devices in the school (where this is allowed). Parents/Carers will also:
- be asked to sign the parent / pupil agreement when they register their children.
- be offered e-safety training/updates to encourage them to support and encourage positive online activities with their children and help them to use the internet safely via the school website and Class Dojo.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? - UK Safer Internet Centre

Hot topics - Childnet International

Parent factsheet - Childnet International

DRAFT

Teaching and Learning

Why internet and digital communications are important:

- The purpose of any technology in school is to raise educational standards, to promote achievement to support the professional work of staff and to enhance the school's management functions.
- The school has a duty to provide students with quality internet access as part of their learning experience. Internet use is part of the statutory curriculum and a necessary tool.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- Pupils will be taught how to work collaboratively using online platforms, which will teach them transferable skills beyond the lesson.
- They will be taught what internet use is acceptable, and what is not, and be given clear objectives for its use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact. This will include using the CEOP icon and reporting tools directly on websites.
- Issues such as Cyberbullying and online safety will be built into the curriculum to encourage self-efficacy and resilience. Some children who have experienced difficulties or with additional needs may need additional support.

Teaching of Online Safety

At Priestsic Primary, online safety is taught throughout each year group within our Computing Curriculum through explicit lessons, and embedded within our curriculum, following Project Evolve. ProjectEVOLVE resources each of the 330 statements from UK Council for Internet Safety's (UKCIS) framework "Education for a Connected World" with perspectives; research; activities; outcomes; supporting resources and professional development materials. In **Key Stage 1**, pupils will be taught to:

Use technology safely and respectfully, keeping personal information private

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

Use technology safely, respectfully and responsibly

Recognise acceptable and unacceptable behaviour

Identify a range of ways to report concerns about content and contact

*By the **end of primary school**, pupils will know:*

That people sometimes behave differently online, including by pretending to be someone they are not.

That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

How information and data is shared and used online

How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

DRAFT

Uses of Technology

E-mail via Office 365

- At Croft Primary School, we feel that access to anywhere learning is important. However, staff have a strict code of conduct to which they must adhere to. On no account is it permitted for staff to give out their personal email addresses or contact details to parents or pupils. Any correspondence via email or any other application should be via the school office who will then forward it onto the member of staff concerned.
- Pupils may only use approved e-mail accounts on the school system (Gmail or Google Classroom) which is filtered and monitored and only allowed during specific lessons.
- Pupils must immediately tell a member of staff if they receive offensive e-mails from their peers during lessons. No emails are allowed from outside the school domain.
- All incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Published content and the school website

 The Croft Primary School website is partially open and can be universally accessed requiring no user name or password. The DSL is responsible for monitoring the site and staff members are responsible for their curriculum and class pages. However, it is the duty of all users to ensure that appropriate material is uploaded. In the unlikely event of any inappropriate material appearing it should be reported directly to the Head Teacher who will take the necessary action. The contact details on the school's website should be the school address. No staff or pupil's personal details will be published.

Publishing pupils' images and work on the Croft Primary School website, and other platforms including, but not limited to Class Dojo

- Written permission will be obtained from parents and carers before any photographs are published on the school website or other platform.
- Photographs that include children will be selected carefully and will not enable individuals to be clearly identified.
- Pupil's full names will be not be used on the school website and other learning platforms.
- Parents should be clearly informed of the school policy on image taking and publishing when joining school, or if there are any updates.

Social networking and personal publishing on the school learning platform

- Croft Primary School will control access to social networking sites and consider how to educate pupils in their safe use. This may not mean blocking every site, but it may need monitoring and educating pupils in the use.
- Croft Primary School will encourage parents to support their children when setting up any age appropriate social networking profile and offer help and guidance. This includes encouraging families to follow the terms and conditions specifying the appropriate age for using sites.
- Pupils are taught and advised to never give out personal details which may identify them or their location.

Managing video conferencing Via Microsoft Teams

- Pupils will be taught how to use Google Meet to communicate safely with their peers and adults in school.
- Pupils will always ask permission from the supervising teacher before making or receiving a videoconference call via(Google Meet).

Managing emerging technologies

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Mobile phones, tablets and associated cameras will not be used in lessons or formal school time except as part of an educational activity.
- Care will be taken with the use of handheld technologies in school which may not have the level of filtering required.

Protecting personal data

 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018, following GDPR guidelines, which can be found on our website https://www.croft.notts.sch.uk/Key_Info/GDPR/

Authorising internet access

- The school will maintain a current record of all staff and pupils who are given access to school IT systems. Parents will be asked to sign and return a consent form.
- At Key stage 1, access to the internet will be by adult demonstration with directly supervised access to specific online materials.
- Any person not directly employed by the school will be asked to sign an

  'Acceptable use of school ICT within Schools' guidance before being allowed to access the internet from the school site.
- All use of the school internet connection by community and other organisations shall be in accordance with the Online Safety policy.

Cyber Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (via The National College).

The school also sends information/leaflets and regularly updates the Online Safety section of the school website on cyberbullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

DRAFT

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Assessing risks

- Croft Primary School will take all reasonable precautions to prevent access to inappropriate material; however, it is not possible to guarantee that unsuitable material will never appear on the school computer.
- Croft Primary School will monitor ICT use to establish if the online safety policy is appropriate and effective.
- Online safety now covers the safety issues associated with information systems and electronic communications as a whole. This not only encompasses the internet but all wireless electronic devices including mobile phones, games consoles, cameras, tablets and webcams. We must also consider the increasing mobility of access to digital technology through this range of mobile devices.
- It is imperative to consider that the issues at hand are not because of the technology but the behaviour around how it is used. It is now a requirement for all schools and academies to ensure that young people are able to use the internet and related communications technologies appropriately and safely.
- "Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile with pupils using technology at an ever earlier age" – Ofsted
- As a school, we follow Project Evolve based on 330 statements from UK Council for Internet Safety's (UKCIS) framework "Education for a Connected World" with perspectives; research; activities; outcomes; supporting resources and professional development materials.

Handling online safety complaints

- Complaints of internet misuse by a pupil will be dealt with by a senior member of staff.
- Any complaints of a child protection nature must be dealt with in accordance with child protection procedures.
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with the schools behaviour policy.

Communicating the policy – Pupils

- Appropriate elements of the e-safety policy will be shared with pupils.
- Pupils will be informed and be aware that the school network and internet use will be monitored.
- Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified.

 Stakeholders

- At Croft Primary School we educate all stakeholders in the safe use of websites. Photographs of children will be carefully selected to minimise the risk of misuse – Parental consent is always obtained. Pupils' full names will not be used with their photograph anywhere online.
- All system users will be informed that the network and Internet use can be monitored.
- All staff will be given a copy of the Online Safety policy and its importance explained.
- All staff will have access to a range of Online Safety training.
- A scheme of work for Online Safety is part of our curriculum, following 'Project Evolve'.
- Safe Internet rules are displayed in a prominent position in classrooms and referred to regularly.
- Emerging technologies will be examined for educational benefits before being used in the classroom by the Computing Lead and Technical staff.
- No removable media is to be brought into school and used on the school system unless absolutely necessary and it has been approved and scanned for viruses.
- Personal data will be recorded, processed and transferred according to the Data Protection Act.
- All staff will ensure that they take full responsibility for any equipment that is issued to them or their class.

DRAFT

- No images of children will be stored on staff personal mobile phones or other devices.
- All staff user names and passwords are confidential and staff should make all effort to ensure that they remain so.
- Staff personal email address should remain confidential and any requests for contact should be directed through the corporate account (office@croft.notts.sch.uk).
- Any confidential material should be encrypted and saved on the school's password protected server.
- USB pen drives should not be used except for exceptional circumstances and only be used when password protected and encrypted.
- Any lost or stolen items with sensitive material should be directly reported to the DPO (Data Protection Officer).
- Virus protection will be updated regularly.

To be reviewed November 2024

DRAFT