The Croft Primary School
On Line Safety Policy

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the 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.

3. Roles and responsibilities

The Governing Body

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

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) are set out in our safeguarding policy.
The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

The IT Lead

The IT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from

potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's IT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: https://www.childnet.com/parents-and-carers

Visitors and Members of the Community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. 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

The school uses Purple Mash to help deliverer the computing curriculum . It contains an online safety module that class teachers will deliver throughout the year and embed into all computing lessons.

The safe use of social media and the internet will also be covered in other subjects where relevant.
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.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website, NSPCC workshop and other guidance leaflets. This policy will also be shared with parents.

.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher.

6. Preventing and addressing cyber-bullying

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.
The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
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.

The school also sends information/leaflets on cyber-bullying 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.
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.

6. Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff and volunteers are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Parents must fill in a consent form in order for children to bring in a mobile phone please see appendix 4

Any breach of the acceptable use agreement by a pupil may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.
If staff have any concerns over the security of their device, they must seek advice from the Headteacher.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying.
All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 3.
This policy will be reviewed every two years by the Headteacher At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Adopted: October 2021

Review Due: October 2022

The Croft Primary School Online Safety Policy
Parental Guidance & Tips 2021

Online Safety Top Tips for Parents and Children

1. Keep the computer in a family area not in the child's bedroom.
2. Use 'child lock' or filter settings on your Web browser to help prevent unsuitable site access by your child.
3. Regularly supervise the sites your child is visiting.
4. Encourage your child to use their Favourites list to access the sites you have approved to prevent accidental entry to unsuitable sites.
5. Discourage your child from using social Networking sites e.g. MSN, Facebook, Bebo etc. to keep them safe from cyber bullying.
6. Teach your child to switch the monitor off or close the laptop lid, then fetch or tell you if something unsuitable appears on the screen.
7. Agree with older children what sites they are allowed to access.
8. Keep all personal details private and be aware of stranger danger.
9. Above all, encourage your child to talk to you about the web sites and electronic devices they are using at home and school

Social Networking

One of the fastest growing areas of internet use today is social networking. There are over 3,000 social networking sites on the internet. This is changing the way that we communicate. On most of these sites, it is incredibly easy to communicate with our friends, in many cases, sharing lots of personal information and photographs.

These common social network sites all have age limits:

- Facebook, Snapchat, Twitter, Instagram, TikTok and Skype have an age limit of 13.
- MySpace set their limit at 14.
- YouTube requires account holders to be 18, but a 13-year-old can sign up with a parent's permission

There are some things to remember when you are surfing the internet.

1. Treat your password like your toothbrush - keep it to yourself!
2. Keep your home address, your phone number or email address off the internet, MSN and chat rooms.
3. Learn to report someone who is behaving badly.
4. Save the evidence - learn to save emails or on-line conversations.

5. Don't retaliate or reply.
6. Always respect others - think carefully about what you are typing.
7. Tell someone you trust if you see something that worries or upsets you.
8. Remember what you have learned in school - use that at home.

Useful Websites and Organisations

There are many helpful websites that can support parents and children .

Ask About Games	Askaboutgames provides a range of advice on how to stay safe online. It also features advice about finding balance during COVID-19.
SafeToNet	The SafeToNet app helps educate children "in-the-moment" by providing real time detection of harmful or concerning content that they may be sharing.
BBC Own It App	The BBC Own It app helps children stop and think before they press the 'send' button.
Childnet	A tool kit to support parents and carers of any age child to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support.
CTIRU	You can report terrorist content they find online through the public referral tool. More information about what to report and what happens when you make a report.
Internet Matters	Internet Matters has created a #staysafestayhome hub. The hub has information about setting devices up safely, age appropriate conversations to have and resources to support families' wellbeing.
Let's Talk About It	Support for parents and carers to keep children safe from online radicalisation.
LGfL	Support for parents and carers to keep their children safe online, including 6 top tips to keep primary aged children safe online.
Net-aware	Support for parents and carers from NSPCC, providing a guide to social networks, apps and games.

Parent Info	Provides support and guidance for parents from leading experts and organisations.
Thinkuknow	Provides advice from the National Crime Agency (NCA) to stay safe online.
UK Council for Internet Safety	Education for a Connect World. A framework to equip children and young people for digital life.

Appendix 1

The Croft Primary School
Acceptable Use Policy For Pupils

Name:	Date:

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons
- I will hand it in at the start of the day and collect it at home time

I agree that the school will monitor the websites I visit.
I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

- I will always use the school's ICT systems and internet responsibly.

Signed (pupil):

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent):

Appendix 2

The Croft Primary School
Acceptable Use Policy
Staff & Volunteers

Name:	Date:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details

I will:

- I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the school will monitor the websites I visit.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will let the designated safeguarding lead (DSL) and IT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's IT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed:

Appendix 3 The Croft Primary School

Online Safety Incident Log

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 4

Dear Parents,

MOBILE PHONES

As you may be aware from the media, the increasing possession of mobile phones by children has led to inappropriate use of text messaging and photo-phones. Whilst we recognise that there may be a place for the use of mobile phones for some of our oldest children – for example if they are travelling to or from school alone – we would like to reiterate that as a general rule we would prefer that mobile phones are **not** brought to school.

If however, you do feel that it is necessary for your child to bring a mobile phone to school we would ask that you complete and return the form below, that the mobile phone is clearly marked with the child's name; is delivered by them at the start of the school day to the Class Teacher and collected by them at the end of the day. No use of the mobile phone will be allowed during the day. If any child is found to be in possession of a mobile phone which has been brought in without permission, or which should have been handed in, it will be confiscated and only returned to the parent or carer of the child.

You are reminded that the school cannot be responsible for any theft, loss or damage to personal property brought into school, howsoever it may be caused.

Your co-operation in this matter is appreciated.

Yours sincerely,

Mrs. J. Millett,
Headteacher.

✂----------

I (name of parent) _____ request that (name of child) _____ be allowed to bring a mobile phone to school because _____

_____

I agree that he/she will hand in this mobile phone to the Class Teacher at the start of the school day and be responsible for the collection of it. I am aware that should he/she be found to be in possession of a mobile phone during the school day then it will be confiscated and only returned to a responsible adult.

I accept that the school cannot be responsible for any theft, loss or damage to the property howsoever caused.

Signed _____ Date _____