# Crawshawbooth Primary School

## Online Safety Policy

May 2025

Mrs Capstick

# Online Safety Policy

## Mission Statement

Crawshawbooth seeks to provide a happy and secure learning environment where a child's natural curiosity is provided with challenges, experiences and opportunities that will enable them to grow into caring, confident and informed citizens of the future.

## Inclusion Statement

In Crawshawbooth all curricular subjects will be taught inclusively to all children regardless of their special needs, race, religion, culture, gender, sexual orientation and their family circumstances.

The Online Safety Policy is part of the School Improvement Plan and relates to other policies.

## Teaching and Learning

The internet and other digital information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teacher and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

### 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 given clear objectives for Internet use.
- Pupils will be educated in the effective use of the web 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 web 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 crosschecking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant web content.

- Pupils will not be allowed unsupervised Internet access.
- Pupils will be taught about the expected appropriate behaviour online and by themselves and others.

Emails

- When available, pupils may only use approved email accounts on the school system. The school currently uses Purple Mash's simulation emails. These messages are sent to the teacher to approve first, once approved they will be sent to the intended recipient.
- Pupils must immediately tell a teacher if they receive offensive email. The children also have the function 'report to teacher' on every email sent if they think it is inappropriate.
- In email communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- Children can also be sent imitations of SPAM emails or inappropriate emails on Purple Mash in a lesson, to teach them how to respond.
- The forwarding of chain letters is not permitted.

## Published Content and the School Website

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office or direct email forms via departmental areas, linked to school email addresses.
The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
Photographs that include pupils will be selected according to whether parents/carers have given permission.
Pupils' full names will not be used in association with photographs anywhere school website or other online space.
Pictures and work will only be shown on the website, Twitter and Dojo if parents/carers have signed the consent form.
Parents/carers will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
A list of where permission has not been obtained by parents/carers is kept in the office and is available to all web administrators.

## 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 and parents/carers 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.
The pupils can publish work on the Purple Mash school blog. This blog is private and posts can only be seen by pupils and staff.

## Managing Videoconferencing and web cam use

When available, videoconferencing and web cam use will be appropriately supervised for the pupil's age. This will most likely be through the use of Teams or Zoom. This will only be used for educational purposes in the aim to teach children about this form of communication.

## 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.
- Pupils must not use personal cameras of any type in school without the permission of the headteacher.
- Staff should note that technologies such as mobile phones with wireless Internet access should not be able to access school WIFI. The school WIFI requires a password and staff and visitors should not be able to use it on their phones. This is because they 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.
- Mobile phones brought to school by the children will be collected and kept in a secure place until the end of the school day.
- Games machines including the Sony Playstation, Microsoft X Box and others have Internet access which may not include filtering. These may not be used in school.
- School retweet 'NOS's Wake up Wednesday' posts about emerging apps and technologies to keep parents informed on how to protect their children at home.

## Protecting personal data

Personal data will be recorded, processed, transferred and made available according to GDPR.

## Cyber-bullying

The internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. These features of the internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Cyber-bulling is bullying through the use of communication technology like mobile phone messages, e mails or websites. This can take many forms for example:

- Sending threatening or abusive text messages or emails, personally or anonymously and through instant messaging service (e.g. WhatsApp)
- Making insulting comments about someone on a website, social networking set (e.g. Instagram/ Facebook/Roblox chat / Minecraft chat) or online diary (e.g. Blog)
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or e mail or an online messaging platform.

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of school time:

- Advise the child not to respond to the message
- Refer to relevant policies e.g. online safety, bullying, behaviour, PSHE
- Secure and preserve any evidence
- Inform the sender's email service provider
- Notify parents/carers of the children involved
- Consider delivering a parent workshop for the whole community
- Consider informing the police depending on the severity or repetitious nature of offence
- If required, inform the Local Authority Online Safety officer.

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff:

- Inform and request the comments be removed if the site is administered externally
- Secure and preserve any evidence

Any complaints and incidents of cyber-bullying will be dealt with in accordance with our Bullying Policy.

<u>Procedures</u>

- The School Computer system's security will be reviewed regularly.
- Virus protection will be updated regularly.
- The school will work in partnership with parents/carers, the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- Filtering is managed in school and can be controlled by the Headteacher and Computing Subject Leader. If staff or pupils discover unsuitable sites, the URL and content must be reported to the Computing Coordinator or to Blue Orange who will add it to the block list on the filter. The filter will block

children from accessing anything inappropriate and the monitoring system monitors what sites users have accessed and what they have searched.

- The filter sends alert emails to the Computing Coordinator's email if any blocked terms are searched. This includes the time, date and user if logged in.
- There are separate filtering platforms for staff and pupil user accounts.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The filter the school have is called 'Exa Surf Protect'. It can monitor content by username.
- 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 Computer use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.
- Online Safety training will be held on a regular basis for both staff and pupils.
- Online Safety is given precedence within the Computing Curriculum and pupils will be taught how to use technology safely and respectfully, and where to go for help and support if they have concerns about any internet material.
- Online Safety advice and materials will regularly be made available to parents/carers.
- 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.
- All users of Computers in the school (staff, governors, children, guests etc) have to sign the AUP which will be stored in the office.
- 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, by any means, for example (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 a Line Manager should be sought first and appropriate professional language should always be used.
- Staff must not use mobile phones or camera phones during teaching time.

Parents / Carers and Children were consulted in May 2010, 20th June 2018 and February 2023. Staff have regular updates in online safety.
The Policy was approved in May 2010 and reviewed and approved in May 2011. The policy was amended, reviewed and approved in May 2012, May 2013, May 2014, May 2015, May 2016, May 2017, May 2018, May 2019 and May 2020, May 2021, May 2022 and May 2023.

The Policy will be reviewed annually or earlier if necessary.

Appendix 1 Smart Rules

| | |
|---|---|
| S | Keep **safe** by being careful not to give out personal information when you're chatting or posting online. Personal information includes your |
| M | |
| A | |
| R | |
| T | |

Appendix 2 Staff Code of Conduct for ICT

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 school information systems may not be used for private purposes without specific permission from the head teacher.
- 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 or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Head teacher.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- 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.

I have read, understood and accept the Staff Code of Conduct for ICT.
Signed: …… Capitals: …… Date: …… Accepted for school: ……. Capitals: …….

Appendix 3 Permission letter for Internet Access

Dear Parent/Carer

The Internet is becoming increasingly important to the way we gather information, communicate with people across the world, work and live.

We believe that the Internet has a contribution to make to your child's education. In order for your child to make use of the school's Internet facilities I need you to give your permission by signing the enclosed "Internet Permission Form".

I would like to take this opportunity to briefly explain some of the steps we have taken to protect our young people from the inappropriate material that does exist on the Internet.

The School connects to the Internet through an Internet Service Provider (ISP) that provides a level of protection from inappropriate material by blocking sites that are known to contain materials that would be offensive to the majority of people.

The school has its own filtering software in place that is tailored to the specific needs of our school. This software is regularly updated.

During lessons, teachers will direct pupils to appropriate Internet material that has been visited beforehand.

The school's Email facility checks messages coming in and out of the school for inappropriate language, images and viruses.

Internet activities are closely supervised and pupils are not allowed access to computers linked to the Internet unless in the presence of a member of staff.

Pupils are taught acceptable behaviour on the Internet and are asked to agree and conform to our Acceptable Use Policy (AUP).

The school, with the support of the Local Education Authority, has made every effort to protect our pupils from inappropriate material. We believe that the education advantages of using the Internet are enormous and various projects have shown the educational benefits of Internet access.

I enclose a copy of our *Acceptable Use Policy* and *Rules for Responsible Internet Use*. I have also included a paper that lists a number of national bodies, and their websites, that advise on the use of the Internet at home.

If you decide to allow your son / daughter to have access to the Internet at school, please complete the enclosed form and return it to me by ….

Yours sincerely
Head teacher

Enclosed: Internet Permission Form, Acceptable Use Policy, Rules for Responsible Use

## Appendix 4 Internet Permission Form

Please complete and return this form to the School as soon as possible.

As part of your son/daughter's study at school there will be times when s/he will need to gain access to the Internet and send and receive Emails. In order for your son/daughter to make use of the school's Internet and Email facilities we require that this form is completed and signed by you and your son/daughter.

### Pupil

As a school user of the Internet, I have read, understood and accept the school's rules on its use. I will use the school equipment in a responsible way and observe all the restrictions explained to me.

Pupil's signature: _____
Date: _____

### Parent or Guardian

As the parent or legal guardian of the pupil signing above, I grant permission for my son / daughter to use Email and the Internet in school. I understand that the school has taken reasonable care to protect its pupils from inappropriate and objectionable materials but that that protection cannot be guaranteed to be 100% successful. I also understand that pupils will be held accountable for their own actions. I accept responsibility for setting standards for my son/daughter to follow when selecting, sharing and exploring information and media.

Parent/Guardian's signature: _____
Date: _____
Pupil's name: _____
Form/class: _____
Home telephone number: _____

Appendix 5 Procedures for dealing with users who deliberately misuse the Internet

The acceptable behaviour of all members of the school community is covered by existing rules of conduct. In the case of pupils these will be within the school rules, and in the case of staff they will be contained in their conditions of service.

The Internet offers an unusual opportunity for unacceptable behaviour in school. This could include:

- Actively searching for inappropriate material including material of a pornographic, racist and violent nature.
- Downloading files without permission
- Infringing copyright
- Playing online games
- Attacking another person's web sites
- Sending bullying emails / SMS text messages to mobiles
- Using unauthorised Chat rooms, Bulletin Boards, User Groups or other area of the Internet.

The school should consider appropriate sanctions for example:

- Temporary or permanent ban on Internet use.
- Disciplinary action in line with existing practices and conditions of service.
- In extreme circumstances the Local Education Authority and / or the Police may need to be involved

Misuse of the school's facility may not only break the school's rules but may also contravene one or more of the following:
The Obscenity Acts of 1959 and 1964
The Protection of Children Act 1978
The Indecent Display Act 1981
The Criminal Justice Act 1988
The Copyright, Designs and Patents Act 1988
The Obscene Publication Act 1989
The Data Protection Act 1998
The Computer Misuse Act 1990

Appendix 6 Using the Internet in lessons and other teaching and learning situations

The use of the Internet offers teachers and pupils many ways to enhance learning activities and provides access to materials that could not be otherwise used in the classroom.

As with all other school activities the use of Internet must be carefully planed and supervised.

## Supervision

Close supervision is the best way of ensuring that pupils are not attempting to visit site inappropriate for the activity in hand.

**Pupils should not be allowed to use the Internet unless they are supervised by a responsible adult.**

All members of staff are responsible for the appropriate use of the Internet within the lessons they supervise.

The staff should make sure that pupils are aware of, and conform to, the School's / Service's rules for the use of the Internet.

All members of staff should be aware of the possibilities of misuse of the Internet, the polices and procedures in place for dealing with such misuse and conduct appropriate supervision.

## Handling Online 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 Online Safety policy in newsletters, the school brochure and on the school website.
- The school will ask all parents to sign the Parent/Pupil agreement as part of the Admissions procedure.