



Online Safety Policy

Approved by:	Children's Committee	Date: 4 th July 2019
Signed by:	(Chair)	
Last reviewed in:	June 2019	
Next review due by:	Summer 2020	

Writing and reviewing the Online Safety Policy

The online safety Policy is part of the School Improvement Plan and relates to other policies including those for Computing, Anti-Bullying and for Child Protection.

For your reference, the schools' 'ONLINE SAFETY OFFICER' is: Mrs N. Beckham

Our Online Safety Policy has been written by the schools' Online Safety Officer/ICT Co-ordinator, building on the existing County Durham Internet Use policy as well as other LEA's E-safety policies and various government guidance. It has been agreed by senior management and approved by governors.

The Policy was revised by: Mrs N. Beckham (June 2019)

**This policy will be reviewed at least annually.
It will also be revised following any concerns and/or updates to national and local guidance or procedures**

Policy Aims

- This online safety policy takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2016 procedures.
- The purpose of Croft Community Schools online safety policy is to:
 - Safeguard and protect all members of Croft Community School community online.
 - Identify approaches to educate and raise awareness of online safety throughout the community.
 - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
 - Identify clear procedures to use when responding to online safety concerns.
- Croft Community School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
 - **Content:** being exposed to illegal, inappropriate or harmful material
 - **Contact:** being subjected to harmful online interaction with other users
 - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

Policy Scope

- Croft Community School believes that online safety is an essential part of safeguarding and acknowledges it's duty to ensure that all pupils and staff are protected from potential harm online.
- Croft Community School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Croft Community School believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.

- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.2 Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
 - Anti-bullying policy
 - Acceptable Use Policies (AUP) and/or the Code of conduct
 - Behaviour and discipline policy
 - Child protection policy
 - Confidentiality policy
 - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)
 - Data security
 - Image use policy
 - Mobile phone and social media policies
 - Searching, screening and confiscation policy

Monitoring and Review

- Croft Community School will review this policy at least annually
 - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

Roles and Responsibilities

- The school has appointed Mrs N. Beckham to be the Online Safety Lead.
- Croft Community School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of conduct and/or an AUP, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement.

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.

- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and AUPs..
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

- Implement appropriate security measures (*including password policies and encryption*) to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the school AUPs.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

It is the responsibility of parents and carers to:

- Read the school AUPs and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and/or AUPs. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school online safety policies.

- Use school systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Teaching and learning

Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high-quality Internet access as part of their learning experience.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments,
- educational materials and effective curriculum practice;

- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with DCC and DfE;
- access to learning wherever and whenever convenient.

Internet use will enhance and extend learning

Increased computer numbers and improved Internet access may be provided but its impact on pupils learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Methods to detect plagiarism may need to be developed.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and pupils.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Education and engagement with pupils

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access.
 - Including online safety in the PSHE, and Computing programmes of study, covering use both at home school and home.
 - Reinforcing online safety messages whenever technology or the internet is in use.
 - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
 - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school will support pupils to read and understand the AUP in a way which suits their age and ability by:
 - Displaying acceptable use posters in all rooms with internet access.
 - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
 - Rewarding positive use of technology by pupils.
 - Implementing appropriate peer education approaches.
 - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
 - Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
 - Using support, such as external visitors, where appropriate, to complement and support the school's internal online safety education approaches.

Pupils will be taught how to evaluate Internet content

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular, it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc. provide an opportunity for pupils to develop skills in evaluating

Internet content. For example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Training and engagement with staff

The school will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
 - This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

Awareness and engagement with parents and carers

- Croft Community School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events and coffee mornings etc.
- Drawing their attention to the school online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our school, for example, within our home school agreement.
- Requiring them to read the school AUP and discuss its implications with their children.

Reducing Online Risks

Croft Community School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.
- All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches.

Safer Use of Technology

Classroom Use

- Croft Community School uses a wide range of technology. This includes access to:
 - Computers, laptops, iPads and other digital devices
 - Internet which may include search engines and educational websites
 - School learning platform/intranet
 - Email
 - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.

Managing Internet Access

The school will maintain a written record of users who are granted access to the school's devices and systems.

All staff, pupils and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet

Decision Making

- Croft Community School governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate,

with consent from the leadership team; all changes to the filtering policy are logged and recorded.

- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

Information system security

- School ICT system security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) security issues include:

- DCC Broadband firewalls and local CPEs are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership between schools and DCC
- The Schools Broadband network is protected by a cluster of high performance firewalls at the Internet connecting nodes in Durham. These industry leading appliances are monitored and maintained by a specialist security command centre.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.

- Files held on the school's network will be regularly checked.
- The Online Safety Lead/ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced

E-mail

In society today email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools in neighbouring villages and in different continents can be created, for example. The implications of email use for the school and pupils need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional school boundaries. A central question is the degree of responsibility that can be delegated to individual pupils as once email is available it is difficult to control. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible. In the school context (as in the business world), email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents/carers, pupils and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

The use of email identities such as john.smith@school.durham.sch.uk generally needs to be avoided for younger pupils, as revealing this information could potentially expose a child to identification by unsuitable people. Email accounts should not be provided which can be used to identify both a student's full name and their school. Secondary schools should limit pupils to email accounts approved and managed by the school. For primary schools, whole-class or project email addresses should be used. When using external providers to provide students with email systems, schools must pay close attention to the sites terms and conditions as some providers have restrictions of use and age limits for their services.

Spam, phishing and virus attachments can make email dangerous. The DCC Network uses industry leading email relays to stop unsuitable mail using reputation filtering.

- Students may only use approved e-mail accounts on the school system. (Currently : Durham accounts set up via Office 365) Personal accounts used at home are not permitted.
- Students must immediately tell a teacher if they receive an offensive e-mail.
- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from students to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- Schools will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- Staff should not use personal email accounts during school hours or for professional purposes.

Websites can celebrate pupils' work, promote the school and publish resources for projects. Editorial guidance will help reflect the school's requirements for accuracy and good presentation. Sensitive information about schools and pupils could be found in a newsletter but a school's website is more widely available. Publication of any information online should always be considered from a personal and school security viewpoint. Material such as staff lists or a school plan may be better published in the school handbook or on a secure part of the website which requires authentication.

School staff are encouraged to 'blog' pupils work, effort and behaviour via the school website so that pupils, parents, carers and the general public can read about it, if and when it happens. All blogs are archived for reference purposes. We believe that our school blog provides a good reference/record of what we

do/achieve at our school. The website can be updated on a daily basis due to the nature of its setup.

- Staff or student personal contact information will not generally be published unless permission has been given.
- The contact details given online should be the school office.
- The headteacher or an appointed nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with the Data Protection Act 1998.

Publishing students' images and work

Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless, the security of staff and pupils is paramount. Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown. Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. "Over the shoulder" can replace "passport style" photographs but still convey the educational activity. Personal photographs can be replaced with self-portraits or images of pupils' work or of a team activity. Pupils in photographs should, of course, be appropriately clothed. Images of a pupil should not be published without the parent's or carer's written permission. Pupils also need to be taught the reasons for caution in publishing personal information and images online

- Photographs that include students will be selected carefully so that individual pupils cannot be identified or their image misused.
- Students' full names will not be used anywhere on a school web site or other on-line space, particularly in association with photographs.
- Student names should not be published with their photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school web site or other school literature. A 'pupil permission list' will be updated on a regular basis (with new pupil intakes) and will indicate if individual pupils have permission for their photo or video footage to be published on school promotional literature (e.g. School website, school prospectus etc.)
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

- As the school blog can be potentially updated on a daily basis all photographs are double checked against the 'pupil permission list' prior to being uploaded.
- All uploaded photographs are copyright protected so that individual photographs can not be copied/pasted easily elsewhere. Parents, Carers and students are reminded that website images are copyright protected and that they should not use images published on our school website on their own personal social networking accounts.

Social networking, social media and personal publishing

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control. For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

- The school will control access to social media and social networking sites, and consider how to educate students in their safe use.
- Pupils are not permitted to access personal social media accounts in school. Access to such sites are blocked by the schools filter system.
- 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 and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Students will be taught about how they should not place personal photos on any social network space without considering how the photo could be used now or in the future.

- Students will be advised on security and encouraged to set 'strong' passwords, to deny access to unknown individuals and to block unwanted communications.
- Students should only invite known friends and deny access to others.
- Staff are not expected to have pupils as part of their own social network and are advised of the inappropriateness of this and the potential dangers.
- Occasionally pupils/parents or carers may attempt to send friend requests/private messages to staff via social networking sites, if this occurs staff should print out a screenshot of the friend request/message and complete a 'School online safety and computer misuse incident log' form with the printout attached. This information will be filed by the Online Safety Officer for future reference if necessary.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and

professional behaviour will be outlined in the school Acceptable Use Policy. Staff use of social networking sites will be readdressed on a regular basis.

Internet Use

- Pupils should seek permission prior to using/accessing the internet
- If pupils are required to use the internet during school time - staff should monitor/supervise their use of it at all times

Managing Filtering

It is important that schools recognise that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. mobile phone). Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that pupils should always be supervised when using internet access and that Acceptable Use Policies are in place. In addition, Internet Safety Rules should be displayed, and both children and adults should be educated about the risks online. There should also be an Incident Log to report breaches of filtering or inappropriate content being accessed.

Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc. just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- The School currently uses a filtering system throughout the school network.
- The school filtering system is used to blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The school will work in partnership with D.C.C., Becta and the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the Online Safety Coordinator (Mrs N. Beckham) or the Network Manager (Mr N. Campbell).
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure. (via school website, staff handbook, lessons etc.)
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Online Safety Coordinator or Network Manager who will then record the incident and escalate the concern as appropriate.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

Managing videoconferencing and or Webcams

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing/use of webcams will be appropriately supervised for the students' age.
- All videoconferencing/webcam equipment in the classroom must be switched off when not in use and not set to auto answer.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Responsibility for the use of the videoconferencing/webcam equipment outside school time will be established with care.

Users

- Parents and carers consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the pupils' age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, the school will check that recording is permitted to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-school site, staff will check that the material they are delivering is appropriate for the class.

Managing emerging technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are

becoming embedded within school systems. Online communities can also be one way of encouraging a disaffected pupil to keep in touch. The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites and other online tools such as Facebook, YouTube, Skype and Twitter.

The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible.

Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details. New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher's reaction in a difficult situation.

Schools should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance, text messaging via mobile phones is a frequent activity for many pupils and families; this could be used to communicate a pupil's absence or send reminders for exam coursework. There are dangers for staff however if personal phones are used to contact pupils and therefore a school owned phone should be issued. The inclusion of inappropriate language or images is difficult for staff to detect. Pupils may need reminding that such use is inappropriate and conflicts with school policy. Abusive messages should be dealt with under the school's behaviour and/or anti-bullying policies.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team acknowledge that technologies such as mobile phones, iPads, Kindles etc. with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. Use of such devices should be supervised at all times. Pupils should seek permission relating to internet use on such devices.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.
- Pupils are not permitted to bring mobile phones into school. (Pupils must hand their mobile phone to the BSU at the start of the school day. It

may be collected at the end of the school day) Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Additionally, pupils are not permitted to use cameras in mobile phones, watches or other hand held devices within the school environment.

- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

Management of Mobile Phones and Personal Devices

Mobile phones and other personal devices such as Games Consoles, Tablets, PDA, MP3 Players etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features. However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render pupils or staff subject to cyberbullying;
- Internet access on phones and personal devices can allow pupils to bypass school
- security settings and filtering.
- They can undermine classroom discipline as they can be used on "silent" mode;
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

Due to the widespread use of personal devices it is essential that schools take steps to ensure mobile phones and devices are used responsibly at school and it is essential that pupil use of mobile phones does not impede teaching, learning and good order in classrooms.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour or bullying policy. The phone or

device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer.

- If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas
- within the school site such as changing rooms, toilets and swimming pools.

Pupils Use of Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining
- body. This may result in the student's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose. Staff should be given clear boundaries on professional use. Staff should not take photographs of pupils on their own personal mobile phones. Staff have now been provided with a classroom iPad or digital camera to record pupils at work/evidence of work/anticipation. All photos taken on these should be uploaded to the school network. All iPad devices should be encrypted in some way to ensure that they cannot be accessed by other users (user code)
- If a member of staff breaches the school policy then disciplinary action may be taken.

Protecting personal data

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that

will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them.

The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Password policy

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.
- From year 7, all pupils are provided with their own unique username and private passwords to access school systems; pupils are responsible for keeping their password private.
- We require all users to:
 - Use strong passwords for access into our system.
 - Change their passwords every year or if they believe somebody else knows it.
 - Always keep their password private; users must not share it with others or leave it where others can find it.
 - Not to login as another user at any time.

Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.

- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

Policy Decisions

Authorising Internet access

- All staff must read the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- All pupils and staff must apply for Internet access individually by agreeing to comply with the 'Responsible Internet Use statement'.

Assessing Risks

- 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. Neither the school nor D.C.C can accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

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.

- Students and parents will be informed of the complaints procedure.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.
- Neither the school nor DCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT/Computing use to establish if the Online Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Responding to incidents of concern

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used. An Online Safety Policy should recognise and seek to develop the skills that children and young people need when communicating and using technologies enabling them to keep safe and secure and act with respect for others. Online Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Staff should also help develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the school Designated Child Protection Coordinator. Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, schools should determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible, after contacting the Children Safeguard Team or Online Safety officer, if the offence is deemed to be out of the remit of the school to deal with.

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, Cyberbullying, illegal content etc.).
- An 'online safety and computer use log sheet' has been created. All staff have access to these forms and they should be completed and returned to the Online Safety officer immediately afterwards an incident has occurred or been observed. Information logged will be followed up by relevant people and findings recorded on the reverse side of the form.
- The Online Safety Coordinator and Behaviour Coordinator will record all reported incidents and actions taken in the School online safety and computer misuse incident log sheet and other in any relevant areas e.g. Bullying or Child protection log. (online safety and computer misuse file)
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage Online-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or Online Safety officer and escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County Online Safety Officer.

Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
 - The DSL will record these issues in line with the school's child protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the D.C.C. Safeguarding procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to online safety.

Procedures for Responding to Specific Online Incidents or Concerns

Youth Produced Sexual Imagery or "Sexting"

- Croft Community School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- Croft Community School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Dealing with 'Sexting'

- If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:
 - Act in accordance with our Child protection and Safeguarding policies and the relevant D.C.C. Safeguarding Child Board's procedures.
 - Immediately notify the Designated Safeguarding Lead.
 - Store the device securely.
 - If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
 - Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
 - Inform parents and carers, if appropriate, about the incident and how it is being managed.

- Make a referral to Specialist Children's Services and/or the Police, as appropriate.
- Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
 - Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.
- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- The school will not:
 - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
 - In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
 - Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

Online Child Sexual Abuse and Exploitation

- Croft Community School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

- Croft Community School recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.
- The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community via the school website.

Dealing with Online Child Sexual Abuse and Exploitation

- If the school are made aware of incident involving online sexual abuse of a child, the school will:
 - Act in accordance with the school's Child protection and Safeguarding policies and the relevant DCC Safeguarding Child Board's procedures.
 - Immediately notify the Designated Safeguarding Lead.
 - Store any devices involved securely.
 - Immediately inform Durham police via 101 (or 999 if a child is at immediate risk)
 - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
 - Inform parents/carers about the incident and how it is being managed.
 - Make a referral to Specialist Children's Services (if required/ appropriate).
 - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
 - Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.

- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
 - Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report : www.ceop.police.uk/safety-centre/
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Durham Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted, the school will seek support from Durham Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.3 Indecent Images of Children (IIOC)

- Croft Community School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Durham Police and/or the Education Safeguarding Team.
- If made aware of IIOC, the school will:
 - Act in accordance with the school's child protection and safeguarding policy and the relevant D.C.C. Safeguarding Child Boards procedures.
 - Immediately notify the school Designated Safeguard Lead.

- Store any devices involved securely.
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Durham police or the LADO.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
 - Ensure that the Designated Safeguard Lead is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the school devices, the school will:
 - Ensure that the Designated Safeguard Lead is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
 - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
 - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
 - Ensure that the headteacher is informed.
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
 - Quarantine any devices until police advice has been sought.

Management of Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobile phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents
- gives headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.
- Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on.
- Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997,
- the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed they should seek assistance from the police.
- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.

- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in cyberbullying may include:

- • the bully will be asked to remove any material deemed to be inappropriate or A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected

Reporting Cyberbullying

- **CEOP Weblink**

Pupils may use the CEOP web link attached to the school website to report any incidents of concern.

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Croft Community School and will be responded to in line with existing school policies, including Anti-bullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Durham Police.

Prevent, Online Radicalisation and Extremism and Counter Terrorism

The internet provides children and young people with access to a wide range of content some of which is harmful. Extremists use the internet, including social media to share their messages. The filtering systems used in our school blocks inappropriate content, including extremist content. We also filter out social media, such as Facebook. Searches and web addresses are monitored and the ICT technician will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found. Where staff, children or visitors find unblocked extremist content they must report it to a member of staff. The acceptable use of ICT policy (AUP) refers to preventing radicalisation and extremist content. Pupils and staff are asked to sign the AUP annually to conform they have understood what is acceptable. Pupils and staff know how to report internet content that is inappropriate or of concern. (update feb. 2016)

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school. If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child protection policy.

If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child protection and Allegations policies

Communicating Online Safety

Introducing the online safety policy to pupils

- Online Safety rules will be posted in all rooms where computers are used.
- Students will be informed that network, email and internet use will be monitored.
- A programme of training in online Safety will be developed, possibly based on the materials from CEOP/Think You Know resource materials.
- We have installed 'Hectors' World Safety Button' on all classroom computers. Pupils have been informed to use this if at any point they find anything deemed to be unsuitable whilst browsing the internet. (By clicking on the 'Hector/Dolphin' icon pupils can prevent/hide others from seeing the site content and alert a member of staff to the individual website. Staff should contact the network manager to block the site if deemed to be inappropriate.

Staff and the Online Safety policy

- All staff will be given access to the School Online Safety Policy and its importance explained (an up to date copy will be available to read on the schools 'shared area' and school website)
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

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 Web site
- Parents and Carers will be made aware of how online safety is taught (Computing project overview, parents evening, website information etc)
- Parents and Carers will be made aware of the pupil acceptable use agreement and School Computing rules.
- The school will maintain a list of online safety resources for parents/carers
- Online safety advice will be offered to parents/carers (for example in-school or via the school website)