Danby CE VC Primary School Online Safety Policy

Effective Date:	May 2018
Date Due for Review:	May 2021
Approved By:	Full Governing Body
Approval Date:	May 2018

Online safety involves pupils, staff, governors and parents making the best use of *Information Communication Technology*. This policy is to create and maintain safe Online safety and ICT environment for Danby CE VC Primary School.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal. "

"The use of technology has become a significant component of many safeguarding issues. Technology often provides the platform that facilitates harm. An effective approach to online safety, empowers a school to protect and educate the whole school in their use of technology and establish mechanisms to identify, intervene and escalate any incident where appropriate."

Keeping Children Safe in Education September 2016

Roles and Responsibilities
Governors:

The Governors are responsible for reviewing the effectiveness of the Online Safety policy.

Mr John Pinkney (Chair of Governor) is the Online Safety Governor responsible for:
- Regular meetings with the Headteacher
- Regular monitoring of online safety logs
- Report to relevant Governor meetings

Head teacher and Staff :
- The Head teacher is responsible for ensuring the safety (including Online safety) of members of the school community.
- The Head teacher is responsible for ensuring that staff receive suitable CPD to enable them to carry out their Online safety roles and to train other colleagues, as relevant.
- The Head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online

safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Head teacher and Deputy Head will follow relevant procedures in the event of a serious Online safety allegation being made against a member of staff.

The Online Safety / Safeguarding Designated Person (Mrs L. Orland) Head teacher:

- Takes day-to day-responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policy / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online safety incident taking place.
- Provides advice for staff
- Liaises with school ICT technical staff.
- Receives reports of Online safety incidents and creates a log of incidents to inform future Online safety developments.
- Attends relevant meetings.
- Is aware of the potential safeguarding issues that may arise from the use of technology.

Teaching and Support Staff:
- Have an up to date awareness of online safety matters and of the current online safety policies and practices.
- Have read, understand and signed the Staff Acceptable Use Policy.
- Report any suspected misuse or problem to the Headteacher.
- Ensure that all digital communications with pupils and their families will be on a professional level.
- Ensure that Online safety issues are embedded in all aspects of the curriculum
- Are responsible for ensuring that students follow the online safety and acceptable use policies
- Are responsible for monitoring the use of digital technologies, mobile devices, cameras etc. in lessons and school activities.
- Ensure that when children are directed to websites as part of their learning they will have been checked for appropriateness by the teacher setting the learning
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Technical Staff:
Danby CE VC School has a managed ICT service provided by North Yorkshire Schools ICT, they are responsible for:
- Ensuring that the technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensuring that the school meets the required online safety technical requirements
- Ensuring that users may only access the networks and devices through a properly enforced password protection policy.

Teaching and Learning:

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- When children are directed to websites as part of home learning they will have been checked for appropriateness by the teacher setting the learning
- Only authorised equipment, software and Internet access can be used within the school.
- Parents are authorised to access the Internet via a password to support a child with their Sumdog program.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in society. The impact of this is regularly monitored by staff.

Safeguarding

The internet opens up new opportunities and is becoming an essential and beneficial part of the everyday world for children. The school will take all reasonable precautions to prevent access to inappropriate material. However, we cannot guarantee that unsuitable material will never appear on a school computer and on occasion, there are inappropriate and undesirable elements that must be managed.

- If staff or children discover unsuitable sites, URL (address), time and content will be reported to the Teacher who will then report to the Headteacher, by recording the incident in an Online Safety Log which is stored in the Headteacher's / School office with other safeguarding materials. The Online Safety Log will be reviewed termly by the Headteacher.
- The school will work in partnership with the Local Authority to ensure monitoring and filtering systems are as effective as possible.

Email:

Email is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of online safety.

- Staff and children who have personal email accounts will not be allowed to access these in school.
- Pupils must immediately tell a teacher if they receive an offensive emails from others.
- Emails sent to external organisations will be written carefully and authorised before sending from the school email address.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding

Social Networking

Social networking Internet sites (such as, Instagram, Facebook etc) provide facilities to chat and exchange information Online safety. This Online safety world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites in the school is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils will be encouraged to only interact with known friends and family over the Internet and deny access to others.
- Pupils will be advised to only play on age appropriate games and understand the dangers of online gaming such as 'x box live'
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Mobile Phones

Mobile phones often allow access to the Internet and digital images being shared. This can lead to the risk of inappropriate contact.

- Pupils may only bring mobile phones to school by prior arrangement with the headteacher. These will be locked away in the school office during school hours.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff will always use the school phone to contact parents.
- Staff may use their mobile phones during periods of non-contact time.
- Staff will use mobile phones to take photographs of the children.

Digital and Video Images (including school website)

There are significant benefits to using digital and video imaging. However, staff/volunteers/students, parents/carers and pupils need to be aware of the risks of publishing digital images on the internet. Digital images may remain on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

- Staff will educate pupils on the risks associated with taking, sharing and publication of digital images.
- In accordance with guidance from the Information Commissioners Office, parents/carers are welcome to take videos and digital images of their children at school events **for their own personal use.** To respect privacy and in some cases protection, these images should not be made publicly available on social networking sites without the specific permission of the parents of the children involved.

- Staff, volunteers and pupils should only take digital images and video in line with school policies.
- Photographs published on the school website or elsewhere that include pupils, will be selected carefully to comply with good practice guidance on the use of such images.
- The full names of pupils will not be used on a website alongside photos of individual children.
- Written permission is obtained from parents before photographs of pupils are placed on the school website or other media which is reviewed annually at the start of each academic year.

Information System Security
- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly
- Security Strategies will be discussed with the Local Authority

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 Head teacher
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Discussions will be held with the community police officer to establish procedures or handling potentially illegal issues.