



Crawford Village
Primary School & Nursery

Small enough to care...big enough to inspire

Online Safety Policy

Introduction

The purpose of this online safety policy is to:

- establish rules for using the Internet and electronic equipment in school
- describe how these fit into the wider context of our behaviour for learning and PSHE policies
- demonstrate the methods used to protect the children from unsuitable material

The benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

At Crawford Village Primary School, we feel that the most effective ways of ensuring responsible Internet use by our children involves a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Why the Internet and emergent technology are important

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 information and business administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use. 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 experiences.

How the Internet benefits education

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in government initiatives;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to e-learning, national developments, educational materials and best curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LEA and Government agencies.
- improved communications between the home and school.

How the Internet can enhance teaching and learning

Internet access at school is designed for pupil use and will include filtering of website content appropriate to the age of pupils. Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use. Internet access is planned to enrich and extend learning activities. Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be

educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.

Evaluating Internet content

Pupils are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy. Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work. As far as possible, Internet searches and website content should be checked by an adult prior to the children using the Internet, especially when search terms may be ambiguous. If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider within the LEA. This is done by reporting any incident to the Headteacher, who will record the incident in an Online Safety Incident Log. Keeping safe online is a regular feature of sessions involving internet access. The subject leader for Computing attends annual e-safety training sessions delivered by the local authority and shares outcomes in staff meetings.

Managing email

Children will have access to email accounts during key stage two. These will be introduced for use in curriculum work when needed. The school's Rules for Responsible Internet Use include the use of email. Pupils must immediately tell a teacher if they receive an offensive email. Pupils are taught never to reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in email communication.

Managing school website content

- Staff or pupils' home information will not be published on the website.
- The website will not mention any pupils by their full name and photographs will be selected carefully so that the full name of individual pupils is not identifiable.
- Written permission from parents or carers will be obtained through the school Internet Access Agreement before photographs of pupils are published on the school website.
- The Headteacher will take overall editorial responsibility and ensure content is accurate and appropriate.
- The copyright of all material that appears on the website must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- It is the responsibility of class teachers to appropriately update class pages.

Internet access and risk assessment

In the Early Years Foundation Stage and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials. In Key Stage Two, children will be expected to carry out focussed searches using the Internet and any work done on the Internet should be done with an adult present. In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor Lancashire Education Authority can accept liability for the material accessed, or any consequences of Internet access. Methods to identify, assess and minimise risks will be reviewed regularly. The Headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored. The following outlines some of the potential risks associated with Internet use:

Area of risk

Examples of risk

Commerce

Pupils should be taught to identify potential risks when using commercial sites.

Advertising
Privacy of information (phishing, identity fraud)
Invasive software (e.g. virus, trojan, spyware)
Online gambling
Premium rate sites

Content

Pupils should be taught that not all content is appropriate or from a reliable source.

Illegal materials
Inaccurate / bias materials
Inappropriate materials
Copyright and plagiarism
User generated content (e.g. YouTube)

Contact

Pupils should be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.

Grooming
Cyberbullying
Contact inappropriate emails / blogs / instant messaging
Encouraging inappropriate contact

Internet filtering

The school will work in partnership with parents, Lancashire LEA, and the DfES guidelines to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL (address) and content must be immediately reported to the Internet Service Provider via the Headteacher. Any material that the school believes is illegal must be referred to the Local Education Authority. All internet devices belonging to school use Internet Content Filtering provided by Lancashire LEA.

IMPORTANT NOTE: It should be noted that the main aim of content filtering is to MINIMISE THE RISK OF USERS ACCESSING INAPPROPRIATE MATERIAL ON THE INTERNET. Whilst the content filtering provision will significantly contribute towards this, it should NOT be viewed as a complete solution that will block all inappropriate material and therefore should be underpinned with good practice at home and at school.

Lancashire LEA operate a devolved filtering system where schools can unblock certain sites at a local level without having to refer the request to Lancashire. This can be useful when sites with good educational content are blocked erroneously. Unblocking a site can only be done with the Headteacher's specific permission. It must also be noted that once a site is unblocked it is unblocked across the entire school, not just on the machine that is being used. A record of staff who unblock websites is kept by the filtering software and it is imperative that the address is blocked once again after it has been used. It is envisaged that this feature of the filtering system will be used sparingly.

Introducing the Internet policy

Rules for Internet access will be posted near all computer systems. Pupils will be kept aware that Internet use will be monitored. Instruction in responsible and safe use should

precede Internet access in each year group. This policy will be made available to parents via the school website.

Staff use of the Internet

All adults who use the school internet system must sign to accept the terms of the 'Acceptable Use' statement before accessing the internet in school. All adults, including teachers, supply staff, classroom assistants and any other adults who may use the internet in school, will be provided with the Online Safety Policy, and its importance will be explained. Staff development in the safe and responsible use of the Internet will be provided as required. They will also be made aware that internet traffic can be monitored and traced **if** there are any concerns about inappropriate use of the internet. Where concerns exist regarding use of the internet, or the accessing of suspected illegal material, these must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF).

Staff must never personally investigate, interfere with or share evidence as this may lead to them inadvertently committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Always report potential illegal content to the Internet Watch Foundation (<http://www.iwf.org.uk>). They are licensed to investigate – schools are not.

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred.

More details on these categories can be found on the IWF website (<http://www.iwf.org.uk>)

Inappropriate use by children

It is more likely that school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence. Equipment such as mobile phones or mobile games consoles should not be brought into school unless asked for by the class teacher

The following table outlines possible incidents alongside procedures and sanctions:

Incident	Procedures and sanctions
Accidental access to inappropriate materials.	Minimise the webpage. Children to tell a trusted adult in the lesson. Report the incident to the Headteacher who will record it in the incident log. Report to LGFL filtering services if necessary. Inform parents / carers.

Deliberately searching for inappropriate materials. Bringing inappropriate electronic files from home. Using chats and forums in an inappropriate way.

Inform Headteacher.
Record the details in the incident log.
Inform parents / carers.
Additional online safety awareness raising lessons.
More serious or persistent offences may result in disciplinary action in line with the Behaviour for Learning Policy.

Inappropriate use by adults

Accessing the internet for **personal use** during lesson time represents inappropriate use of the internet by adults. Such instances should be reported to the Headteacher who will investigate this issue. Outside of lesson time, such as at dinner time or after school, adults wishing to access the internet for personal use must only access sites which would be deemed appropriate for public consumption. If extended personal use of the internet is required, they must first discuss this request with the Headteacher.

Social networking by staff

Social networking is an increasingly popular way of communicating. When using social network sites, such as Facebook, Instagram or Twitter, members of staff need to be aware of the following good practice:

- They should not willingly allow access by pupils or parents/carers to their social network accounts which may show personal content that could be considered to be unprofessional.
- Adults must not communicate with pupils using any digital technology where the content of the communication may be considered inappropriate or misinterpreted.
- Pupils should not be added as 'friends' on staff Facebook accounts and should not be able to access the content of other social network accounts belonging to staff.

Staff need to take into account that whatever the means of communication used, they should always conduct themselves in a professional manner.

Staff email accounts

All members of staff have a school email account to enable professional communication via this medium. They should not use this for personal emails and, equally, should not use personal email accounts for work-related emails.

How will computing system security be maintained?

The school computing systems will be reviewed regularly with regard to security. Virus protection will be installed and updated regularly by the ICT technician.

Handling Internet related complaints

Any incidents of inappropriate Internet use or of accessing inappropriate content must be referred to the Headteacher. Any complaint about staff misuse must be referred to the Headteacher. If the incident relates to use by the Headteacher, this should be referred to the Chair of Governors (contact details available from the school office and on the school website). Pupils and parents will be informed of the complaints procedure. Parents and

pupils will need to work in partnership with staff to resolve any issues that may arise. Any deliberate misuse of the internet may result in withdrawal of access.

Personal devices

Staff may connect their own personal devices, such as mobile phones or tablets, to the school internet connection via the WiFi. Internet access through this connection is then subject to the Internet Content Filtering provided by Lancashire LEA.

Involving parents

Parents' attention will be drawn to the Online Safety Policy in newsletters and on the school website. Any concerns regarding online safety will be handled sensitively to inform parents without undue alarm. A partnership approach with parents is encouraged. This includes demonstrations, practical sessions and suggestions for safe Internet use at home.

Updating the policy

This Online Safety policy has been written by the school, building on Local Authority guidance and government guidance. It has been approved by governors.

PREVENT

The Counter Terrorism and Security Act 2015, section 26th February 2015 places a legal duty by the DfE on schools to have due regard to the need to prevent people from being drawn into terrorism or be subject to radicalisation. In line with legislation to prevent possible radicalization of individuals, the school safeguards children through adherence to the school child protection policy and allowing Internet access only under staff supervision.

Written by: Debra Eaton (Headteacher)

Date: October 2017

Updated October 2018

Review date: October 2019