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, 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 students with quality Internet access as part of their learning experience.

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 will 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 on-line 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 online safety training sessions delivered by the local authority and shares outcomes in staff meetings.

Managing e-mail

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 e-mail. Pupils must immediately tell a teacher if they receive an offensive e-mail. Pupils are taught never to reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail 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 on-line

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

Filtering & Monitoring

The school filtering and monitoring provision is agreed by the Headteacher, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist

knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility

- the filtering and monitoring provision is reviewed annually by the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.
- checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of the Designated Safeguarding Lead, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access

Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school protects users and school systems through the use of the appropriate blend of strategies, including:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed

- *filtering logs are regularly analysed and breaches are reported to the Headteacher*

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 School Internet 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). The

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 (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. 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 maybe 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 that is 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 ICT system security be maintained?

The school ICT 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 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 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 School Internet Policy in newsletters and on the school website. Internet issues 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.

Addendum to Policy in response to COVID-19 Pandemic

Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- No 1:1s, groups only
- Staff and children must wear suitable clothing, as should anyone else in the household
- Any computers used should be in appropriate areas, for example, not in bedrooms
- The live class should be recorded so that if any issues were to arise, the video can be reviewed
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day
- Language must be professional and appropriate, including any family members in the background
- Staff must only use platforms agreed by Crawford Village Primary School
- Staff should record, the length, time, date and attendance of any sessions held

Date: April 2015
Updated 12/10/15
Reviewed: April 2017, 2018, 2019, 2020, 2021, 2022, 2023
Next review: October 2024