Cromwell Academy Online Safety Policy

Introduction

This online safety policy is to ensure everyone has the chance to develop a set of safe and responsible behaviours that will enable them to reduce the risks whilst continuing to benefit from the opportunities that are available from using the Internet and new technologies. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put users at risk; these risks can be categorised into three main areas:

- **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.

We always aim to keep our pupils safe whilst encouraging them to fulfil their potential.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, work placement students, visitors), who have access to and are users of school ICT systems, both in and out of school.

The school will identify within this policy how incidents will be managed and will, where appropriate, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any illegal content or material that could be used to bully/harass others or cause harm.

Good Habits

Online Safety depends on effective practice at several levels:

- responsible ICT use by all staff and pupils, encouraged by education and made explicit through published policies;
- sound implementation of online safety policy in both administration and curriculum, including secure school network design and use;
- safe and secure broadband from the local Grid for Learning, including the effective management of content filtering;
- national education network standards and specifications;
- Pupil data to be kept within the secure network. To enable staff to work from home, data should only be taken from the building electronically, using encrypted software (mainly using an encrypted flash drive).

Policy Implementation

As the roles overlap, the Headteacher is both the online safety co-ordinator and the designated child protection officer, although responsibility may be delegated to a Senior Leader or designated member of staff in charge of Online Safety: Sophie Harrison.

Our online safety policy has been written by the school, building on government guidance. It has been agreed by the senior leadership team and approved by governors.

The online safety policy will be reviewed annually.

Why is Internet Use 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 administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element of 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils, who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How Internet Use Benefits Education

Benefits of using the Internet in education include:

- access to world-wide educational resources, for example; museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;

- education and cultural exchanges between pupils world-wide;
- 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 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 CYPS and the Department for Education;
- access to learning wherever and whenever convenient.

How Internet Use Enhances Learning

Internet use enhances learning by:

- ensuring access is designed expressly for pupil use and includes filtering appropriate to the age of pupils;
- teaching pupils what is and what is not acceptable and giving clear objectives for Internet use;
- planning Internet access to enrich and extend learning activities;
- guiding pupils in online activities that will support learning outcomes planned for the pupils' age and maturity;
- educating pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

Parents will be informed that pupils will be provided with supervised Internet access.

Staff will be made aware of the online safety policy and Internet usage through the induction process.

World Wide Web

If staff or pupils discover unsuitable sites, the URL (address), time and content must be passed onto the online safety co-ordinator or network manager.

School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.

Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

Pupils may only use approved email accounts on the school's internal system.

Pupils must immediately tell a teacher if they receive offensive email.

Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.

Whole class or group email addresses should be used in school.

Access in school to external personal email may not be used by pupils.

The forwarding of chain letters is not permitted.

Social Networking

The school has blocked/filtered access to social networking sites and newsgroups unless a specific use is approved.

The pupils will be advised never to give out personal details of any kind which may identify them or their location. The pupils should be advised not to place personal photos on any social network space.

The pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

Pupils should be encouraged to invite known friends only and deny access to others.

Mobile Phone Use

Pupils are not allowed to use mobile phones in school. Any exceptions to this are by arrangement with the Headteacher and parents. Any phone brought to school must be switched off and handed to the class teacher for safekeeping. It is the child's responsibility to ensure they collect their mobile phone at the end of the school day.

Laptops and devices are provided and maintained by the school for staff use. Staff are not permitted to use personal devices during lesson time. This includes the use of personal devices to take photographs or access the internet for educational purposes or otherwise.

Staff members will be provided with an iPad to take photographs for educational purposes when required.

Filtering
The school will work in partnership with the Internet service provider to ensure filtering systems are as effective as possible. The school network should be contact if issues with filtering arise.

Managing Emerging Technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
If the school becomes aware of any emerging technologies that raise concerns outside of school, this will be communicated with parents and pupils to promote safe use.

Published Content and the School Website
The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work
Written permission from parents or carers will be obtained before photographs of pupils are published on any public domain.
Published photographs that include pupils will be selected carefully according to these parental permissions and considering safeguarding.
Pupils' full names will not be used anywhere on the website or blog, particularly in association with photographs.

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 advisors.

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

Assessing Risks
The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the local council can accept liability for the material accessed, or any consequences of Internet access.
The school will audit ICT use at least annually to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

Handling Online Safety Incidents and Complaints
Complaints of Internet misuse will be dealt with by a senior member of staff and fully investigated in line with the school behaviour and safeguarding procedures (where applicable).
Any complaint about staff misuse must be referred to the Headteacher.
Pupils and parents will be informed of the complaint's procedure.
Discussions will be held with the Police Youth Crime Reduction Officer or Community Police Officer to establish procedures for handling potentially illegal issues.

Responsibilities

Internet safety is the responsibility of all members of the school community.

Pupils:

Rules for Internet access will be made explicit and adhered to by all.

Pupils will be informed that Internet use will be monitored.

Pupils will be required to sign an Acceptable Use Agreement.

Staff:

All staff will be given the school Online Safety Policy and its importance explained annually and at the point of induction.

Staff should be aware that Internet traffic can be monitored and traced to the individual user.

Contribute to the development of Online Safety policies.

Adhere to acceptable use policies.

Take responsibility for the security of data.

Develop an awareness of Online Safety issues, and how they relate to pupils in their care.

Model good practice in using new and emerging technologies.

Include Online Safety regularly in the curriculum.

Deal with Online Safety issues they become aware of and know when and how to escalate incidents.

Maintain a professional level of conduct in their personal use of technology, both within and outside school. Take responsibility for their professional development in this area.

Parents:

Discuss Online Safety issues with their children, support the school in its Online Safety approaches and reinforce appropriate behaviours at home.

Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Model appropriate uses of new and emerging technologies.

Liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online.

Headteacher:

Responsible for Online Safety issues within the school but may delegate the day-to-day responsibility to a Senior Leader as the Online Safety co-ordinator.

Ensure that the Online Safety co-ordinator is given appropriate time, support, and authority to carry out their duties effectively.

Ensure that developments at Local Authority level are communicated to the Online Safety co-ordinator.

Ensure that the Governing Body is informed of Online Safety issues and policies.

Ensure that appropriate funding is allocated to support Online Safety activities throughout the school.

Designated Online Safety Staff:

Primary responsibility: establish and maintain a safe ICT learning environment (under the direction of Senior Management).

Establish and maintain a school-wide Online Safety programme.

Develop and review, Online Safety policies and procedures.

Respond to Online Safety policy breaches in an appropriate and consistent manner in line with protocols set out in policies and maintain an incident log.

Establish and maintain a staff professional development programme relating to Online Safety.

Develop a parental awareness programme.

Develop an understanding of relevant legislation and take responsibility for their professional development in this area.

Governors:

Governors will monitor and review policies relating to online safety annually.

Appoint an Online Safety Governor who will ensure that Online Safety is included as part of the regular review of child protection and health and safety policies.

Support the Head Teacher and/or designated Online Safety coordinator in establishing and implementing policies, systems, and procedures for ensuring a safe ICT learning environment.

Ensure that appropriate funding is authorised for Online Safety solutions, training and other activities as recommended by the Head Teacher and/or designated Online Safety co-ordinator (as part of the wider remit of the Governing Body with regards to school budgets).

Network Manager/Technical Support Staff

Provide a technical infrastructure to support Online Safety practices.

Ensure that appropriate processes and procedures are in place for responding to the discovery of illegal materials, or suspicion that such materials are, on the school's network.

Ensure that appropriate processes and procedures are in place for responding to the discovery of inappropriate but legal materials on the school's network.

Develop an understanding of relevant legislation.

Report network breaches of acceptable use of ICT facilities to the Head Teacher and/or the Online Safety co-ordinator.

Take responsibility for their professional development in this area.

Wider School Community

This group includes: non-teaching staff; volunteers; student teachers; other adults using school internet, Learning Platform or other technologies.

Adhere to acceptable use policies.

Take responsibility for the security of data.

Develop an awareness of Online Safety issues, and how they relate to pupils in their care.

Model good practice in using new and emerging technologies.

Know when and how to escalate Online Safety issues.

Maintain a professional level of conduct in their personal use of technology, both within and outside school.