

Cauldwell Lower School



E-SAFETY POLICY

January 2011

Review Spring Term 2012

E-SAFETY

Rationale

The school encourages use by pupils of the rich information and interactive resources available on the internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills are fundamental in the society to which our pupils belong.

On-line services open classrooms to a broad array of resources. In the past, teaching and library materials could usually be carefully chosen. All such materials would be chosen to be consistent with national policies, supporting and enriching the curriculum while taking into account the varied teaching needs, learning styles, abilities and development levels of the pupils. Internet access, because it may lead to any publicly available site in the world, will open classrooms to electronic information resources which have not been selected by teachers as appropriate for use by pupils.

Electronic information research skills are fundamental to the preparation of citizens and future employees. The school expects that staff will investigate possibilities and blend use of such information as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the appropriate use of such resources. Staff will consult the IT co-ordinator for advice on content, training and appropriate teaching levels consistent with the school's IT programme of study (Smart Learning). Any content to be used as part of the Creative Curriculum.

Access to on-line resources will enable pupils to explore thousands of libraries, databases and activities while exchanging messages with people throughout the world. The school believes that the benefits to pupils from access to information resources and increased opportunities for collaboration exceed the disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information resources. To that end, the school supports and respects each family's right to decide whether or not to allow pupils internet access within the school environment.

School Procedures Resource Development

In order to match electronic resources as closely as possible to the national and school curriculum, teachers need to review and evaluate resources in order to offer materials that are appropriate to the age range and ability of the group being taught. The class teacher will provide appropriate guidance to pupils as they make use of the internet to conduct research and other studies. All pupils will be informed by staff of their rights and responsibilities as users, before their first use, either as an individual user or as a member of a class or group.

While pupils may be able to move beyond those resources which have been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. Pupils may not pursue electronic research independent of staff supervision. The schools internet access is controlled by filtering software chosen by Bedford Borough Council, which should stop access to many inappropriate sites, although we recognise that no system is totally secure.

The staff are aware that all inappropriate sites accidentally accessed in school should be reported to the ICT Co-ordinator, Head teacher and then to Bedford I.Tec.

School Rules

The school has developed a set of guidelines for Internet use by pupils. These rules will be made available to all pupils and kept under constant review.

All members of staff are responsible for explaining the rules and their implication. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils.

All pupils will be taught to five basic rules for internet safety at home, including:

1. Set your privacy settings to friends only and check them regularly
2. Never post a photo that is accessible to all
3. Never reveal personal details
4. Do not add as a 'friend' anyone you don't know
5. Know how to report abuse

Pupil Guidelines for Internet Use

General

Pupils are responsible for good behaviour on the internet just as they are in a classroom or a school corridor. General rules apply.

The internet is provided for pupils to conduct staff guided research and communicate with others. Parents' permission is required. Remember that access is a privilege, not a right and that access requires responsibility. Individual users of the internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with school standards and will honour the values the school holds. The school may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or disks will always be private.

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear responsibility for such guidance, as they must also exercise with information sources such as television, telephones, films, radio and other potential offensive media.

The following will not be tolerated:

- Sending or displaying offensive messages or pictures
- Using obscene language
- Harassing or insulting others
- Damaging computers, computer systems or computer networks
- Violating copyright laws by downloading copyrighted items
- Using others' passwords
- Trespassing in others' folders, work or files

Sanctions

Violations of the above rules will result in a temporary or permanent ban on internet use in school. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

Pupils' internet Safety Rules

RULES FOR ONLINE SAFETY AT CAULDWELL SCHOOL

1. I will always ask the teacher before I use the Internet and will be sensible whenever I use it.
2. I will only use the Internet for schoolwork and will only use the sites my teacher has asked me to access.
3. I will not give my name, address or telephone number to anyone on the Internet and I will tell the teacher if anyone asks me for my name, address or telephone number.
4. I will never agree to meet someone I have spoken to on the Internet.
5. I will not download programmes or bring programmes on disc or CD Rom from home into school.
6. I will only e-mail the people my teacher has approved and the message I send will be polite and responsible.
7. I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself.
8. I realise that if I don't use the Internet sensibly I will not be allowed to use it.

Acceptable Use Policy

The requirement to ensure that pupils, staff and all others in the school community are able to use the internet and related communications technologies appropriately and safely is part of the wider duty of care to which all who work in schools are bound. This framework of e-safety, or acceptable user policy (AUP), is to promote safe and appropriate use. As such, it should be understood in the context of other 'child protection' and 'behaviour' policies that the school already has in place as well as other existing policies in respect of its employees.

Given the glittering array of new technologies now available to use for educational purposes and in everyday life, the intention of this evolving policy is:

- To maximise e-safety for all members of the school community
- To help everyone understand the potential risks
- To provide guidelines (including how the policy will be regulated and any sanctions) for safe and appropriate school and home use.

As such, the school more specifically intends:

- To provide a secure network for the school and secure means of home/school access
- To monitor traffic, log incidents and act accordingly
- To establish key standards and behaviour for e-safety across the school, in keeping with those of the Local Authority
- To co-ordinate the activities for the school related to promoting best practice in e-safety, including the publication of guidelines and acceptable use policies for pupils, staff, parents and governors
- To ensure that we adhere to e-safety issues related to new government policies affecting schools
- To monitor the school's response to e-safety matters and act accordingly
- To have a named Senior Information Risk Officer - (SIRO) – to co-ordinate the development and implementation of e-safety policies, with clear designated responsibilities and liaise with the Local Authority in such matters.

E-safety is a whole-school issue, not something that is simply the responsibility of the ICT co-ordinator. As such, the whole school has a responsibility to promote it.

Guidelines

The AUP aims to:

- Reflect the understanding that all members of the school community have responsibilities towards themselves, towards others and towards the school and that these responsibilities are not confined to the physical location of the school.
- Enable young people to develop their own protection strategies when adult supervision and technological protection are not available.
- Provide information on where to seek help and how to report incidents.
- Help young people understand that they are not accountable for the actions that others may force upon them, but that there are sanctions that the school will impose if they act inappropriately when online.
- Provide guidelines to parents, carers and others on safe practice.
- Ensure that the practice that it promotes is regularly monitored and reviewed with stakeholders.
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.

Strategy

This policy is the result of ideas discussed by the school community. The policy has been put to the school staff and ratified by the Governors. Parents are informed through the home/school agreement, guidelines distributed during Parents' Evening and the pupils' AUP which is signed by them and their children at the beginning of the school year. E-safety guidelines are displayed in the computer areas.

Passwords

Staff and pupil passwords are kept private and only the holder can change them. It is accepted that from time to time, e.g. forgetting a password, the ICT co-ordinator can help to create a new password but s/he will not know what it is. Computers must not be left in 'logged on' mode. It is good practice for users to change their passwords regularly.

Emails

It is accepted that staff may send emails and attachments to recipients outside the school. Children may only do so under the supervision and direction of the teacher.

Anti-virus and anti-spam system

The school has an up to date anti-virus and anti-spam system provided by the Local Authority which is updated weekly. The network is set up to automatically scan laptops and other portable devices every time they are connected to the school system.

Video Conferencing

Under the direct supervision of a teacher/TA children may participate in video-conferencing with other schools.

Restricted (Named staff only)	Protected (All in school community)	Public (Anyone)
Any information that identifies an individual	Routines, management information	Website, parentmail, display

Access to all ICT systems shall be via logins and passwords. Any exception must be SIRO approved. All information storage shall be restricted to necessary users with any additional access being SIRO approved. The SIRO must maintain a record of who has access to restricted information.

Inappropriate content and language

There will be zero tolerance to the use of inappropriate content and language on any ICT equipment within our school community.

The type of language that is used in emails should be no different to that which is used in face to face situation.

Inappropriate Web content:

Chat rooms/instant messaging (except that promoted by the school for educational purposes).	Newsgroups/forums (except that promoted by the school for educational purposes).
Downloads of ring tones, screensavers and games (except promoted by the school for educational purposes)	Internet peer to peer networks
Downloads of freeware, shareware, evaluation packages (except by authorised persons and in compliance with copyright law).	

Staff

The school aims to establish a clear understanding of the responsibilities of all those involved in the education of children and young people with regard to e-safety during staff training sessions. It is expected that all staff will read (and if necessary seek clarification) all school policies. Working at this school means acceptance of those policies including this AUP.

As such:

- Staff must not allow any emails between themselves and pupils to be anything other than school business.
- Staff must not have any pupil (or former pupils) as 'on-line' friends if they are of school age. Staff must report to the SIRO any contact from a pupil or former pupil of school age.
- During ICT lessons pupils should be made aware of the procedures for reporting accidental access to inappropriate materials. In any instance of deliberate misuse the SIRO must be informed and the pupil will be dealt with in accordance with the school's behaviour policy.
- The school email accounts may be used for personal use.
- Staff need to be aware that conducting any personal transaction could result in residual information remaining on the hard drive which may be accessible to others. **Neither the school nor the Local Authority can accept any liability for resulting loss or damage.**
- Staff should keep to a minimum any data which is held on their school laptop and they must lock it if it is left unattended (ctrl + alt + delete, lock). The security of school laptops out of school lies with the staff who, by taking them off school premises, accepts responsibility for them.
- PC's and laptops for pupils must be arranged in classrooms to allow good teacher supervision.
- It is not appropriate for staff members to use personal digital cameras or camera phones on field trips. Images should be transferred onto the school system under the direction of the ICT co-ordinator (refer to school policy about photographs).
- All photographs containing children must be stored on the school network by the ICT Co-ordinator who will arrange for the deletion of them within two years of the child leaving unless parental permission has been given to retain them longer (e.g. for publicity purposes).
- Any restricted data that is taken away from the school premises must be securely encrypted on school devices and only accessed on those devices. Restricted

data must be backed up the Network Manager on a drive specifically set up for this purpose.

- Exporting SIMS data must only be on school devices.

Pupils

Pupils are involved, through the School Council and the work done in ICT lessons in which activities to promote good practice and internet safety issues are delivered, in the evolution of this AUP and the following guidance:

- Pupils are not encouraged to bring into school personally owned devices unless they have been requested by their teacher. Any such device should be handed into the school office for safekeeping until such a time as they are required or collected at the end of the school day.
- The school cannot accept any responsibility for personally owned devices (e.g. laptops, USB devices, external hard drives, mobile phones and digital cameras) brought into school or taken on educational visits. If these are to be used on the school network they must, on a daily basis, first be virus checked by the ICT co-ordinator before they are connected or used. They can only be taken on educational visits at the discretion of the teacher in charge and provided that pupils agree to use them appropriately as they would in school.
- School data should not be stored on these devices other than for the time it is actually being used.
- The VLE should be used as the means for accessing such data off school premises.
- The school accepts the use of school email addressed by pupils in other schools providing they adhere to the pupil AUP.
- Pupils learn about the good practice that is appropriate for social networking through the use the blogging facility on the school network to which they are introduced during ICT lessons.
- Pupils are made aware of the procedures for reporting accidental access to inappropriate materials.

If children accidentally find inappropriate material they are to report it to their teacher who will alert the SIRO so that she can take steps to rectify this. Staff who find inappropriate material will report it directly to the SIRO. Children learn of this procedure in their lessons and it is reinforced. Staff are made aware of their responsibilities in this during staff training and by having their own copy of the policy.

Sanctions

Pupils who deliberately abuse the AUP will be dealt with in line with the school's Behaviour Policy. Parents must be informed and any incident must be logged in school by the SIRO.

This policy will be reviewed within one year of its first ratification by the school Governors.