ICT Acceptable Use Policy

Isleham Church of England Primary School

September 2024

Introduction

This policy outlines the school's views on what is the acceptable use of ICT hardware within school. This policy was drawn up after consultation with staff about what is deemed to be acceptable use. It will be reviewed annually by the ICT Subject Leader, staff and Governing Body. The implementation of the policy is the responsibility of all the staff and is monitored by the ICT Leader, the Headteacher and the Governing Body. All staff are made aware of this policy on an annual basis. The policy is included within the Induction Pack for new staff and Information Pack for supply staff, students and volunteer workers at the school. It is also shared with parents/carers and community users if they have reason to be using the school's ICT facilities e.g. whilst participating on an ICT course.

Ensuring safe and appropriate internet access

We aim to take every practical measure to ensure that pupils do not encounter upsetting, offensive or otherwise inappropriate material on the Internet. The following key measures have been adopted to ensure that our pupils are not exposed to unsuitable material:

- We subscribe to an internet service through Cambridgeshire Schools ICT Service. This incorporates a strict filtering system, which is updated regularly, intended to prevent access to material inappropriate for pupils.
- A smoothwall update is provided weekly, to the SLT to review
- Pupils are supervised by an adult at all times when using the Internet.
- Staff check that the sites pre-selected for pupil use are appropriate for the age and maturity of the pupils.
- All staff understand the vital role they play in protecting pupils from the risks of extremism and radicalisation. Keeping children safe from risks posed by terrorist exploitation of social media is approached in the same way as safeguarding children from any other online abuse. Staff are vigilant about the risks and signs of possible radicalisation and understand the school's safeguarding procedures in relation to PREVENT duty.
- Through the ICT curriculum, pupils are taught to use email and the Internet responsibly in order to reduce the risk to themselves and others.
- Rules for responsible Internet Use are posted in classrooms.

- The ICT Leader monitors the effectiveness of Internet access strategies.

- The Headteacher ensures that this policy is implemented effectively.

- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material are reviewed in consultation with colleagues from other schools and advice from the LA, our Internet Service Provider and the DfE.

Time and experience has demonstrated that the above measures have been highly effective. However, because of the international scale and the nature of the information available via the Internet, it is impossible to guarantee that particular types of material will never appear on a computer screen.

Neither the school nor Internet provider can accept liability for the material accessed, or the consequences thereof.

An important element of our Rules of Responsibility is that through their ICT lessons focusing on e-safety, pupils will be taught to immediately switch off their monitors and tell a teacher if they encounter any material that makes them feel uncomfortable.

If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will swiftly respond to the situation on a number of levels.

Responsibility for handling incidents involving pupils are dealt with by the ICT Leader and a Designated Senior Person for Safeguarding in consultation with the Headteacher and the pupil's class teacher. If appropriate all staff will be made aware of the incident.

• If one or more pupils discover inappropriate material, our first priority is to give them appropriate support. The pupil's parents/carers are informed and given an explanation of the course of action the school has taken.

• If staff or pupils discover unsuitable sites, the ICT Leader is informed and will then ensure the site is blocked by adding it to the list on the filtering service.

The school has a comprehensive E-Safety Policy which outlines in detail the benefits and opportunities of using ICT and how we actively minimise any associated risks. The E-Safety Policy complements this ICT Acceptable Use Policy.

Photographs and digital video

Photographs or videos of pupils to be used as educational evidence are only taken (preferably) using one of the school's digital cameras/video cameras/iPads. If a personal device is used, these photographs/video image, are deleted as soon as possible. The school obtains parental consent to take photographs/videos on admission. Staff are only able to use personal cameras/iPads after seeking permission from the Headteacher. This will only be granted in exceptional circumstances. Images are only downloaded into a file on the staff only drive on the school network. This is done immediately in the case of photos taken on personal devices and are then deleted from the device. Schools staff may have photos temporarily downloaded onto secure drives for assessment purposes e.g. reports/ website upload which are accessed via their own computers. Permission is sought from the headteacher for this and once the photos have been used, they are deleted from personal computers and stored on the school's G: staff share drive.

Unless used on the school website or kept in evidence files on the Staff Shared drive, photographs or videos stored on the network for two years are deleted by each class teacher at the end of the academic year. Staff are able to use mobile phones to photograph or video pupils when on a visit or within the classroom, provided they are saved onto a suitable drive at school, and then deleted, within 48 hours.

Photographs published online or in printed matter are carefully selected so that pupils cannot be identified or their image misused. Only the first names of pupils are used on the website; no names are used in association with any photographs. In exceptional circumstances, for example to celebrate outstanding achievement, and with the agreement of the Headteacher or Chair of Governors and with written permission from a parent/carer, additional information such as a name with a picture may be published.

Acceptable Use for staff

• Staff may use the computers for any purpose relating to their position within school i.e. researching topics to be taught, writing policies, communicating with other educational staff etc.

• School computers should not be used for personal interests of an acceptable nature during the hours of the normal school day. i.e. Internet shopping, banking, booking holidays etc,

• At no time, should the school computers be used to support inappropriate personal interests.

• All staff should log on with their own user name and password as outlined in the password policy.

• Staff should only download material to school computers that is directly related to their post within school. i.e. unit plans, lesson resources, educational documents etc.

• Material for personal use should not be downloaded at any time.

• New software should be checked with the ICT Leader to ensure it is safe and compatible before it is downloaded / installed.

• Staff should not access social networking sites using the school network. Staff should not access social networking sites during the working hours of the school day on their personal devices. Under no circumstances should staff communicate with students or pupils through social networking sites at any time. Improper use of social media by a member of staff could amount to gross misconduct even if carried out via personal social media in the member of staff's own time. Staff will not discuss or comment upon school business on social networking sites. (Some staff may be personal friends with parents/carers and may wish to communicate through social networking sites in their own time, this is acceptable but under no circumstances must school business be discussed or made reference to). Any staff who make reference to specific school business will face disciplinary action. Misuse can qualify as grounds for dismissal.

• Staff are able to bring mobile phones to school. However these devices should not beon show or used during the working day; personal use can only occur during designated break times. Staff should seek permission from the headteacher if a call needs to be taken/made during the working day on a personal mobile; this should be for exceptional reasons only.

Staff can only use personal mobile phones for emergency purposes during the working day whilst taking part in off-site school visits, or when using the school swimming pool.

• Staff should take responsibility for their own personal data devices such as USB memory sticks. They are expected to keep their virus software up to date to minimise risk to the system. Where possible staff are encouraged to email information to themselves or to remotely log into the system when working at home.

Acceptable Use for pupils

• Pupils are made regularly aware of the rules of using the computers. (These are displayed near every machine.)

• Pupils are supervised at all times when using the Internet.

• Pupils in KS2 may have their own personal log on. They should, whenever possible, use this to log in each time they access the school system.

• Pupils may not bring in information on data devices such as USB memory sticks – if they need to access a personal file on the school network at school, for example homework, then they should email it to their class teacher via the school office, class dojo or access it via a secure online or cloud-based storage site.

• Pupils should only log on to the student areas of the school network. Teacher or administrator passwords should never be made known to pupils. If in the rare case a child needs to access something in these areas, a member of staff should save a copy of the file into the student area of the drive.

Acceptable use of laptops/iPads borrowed from school

• Laptops/iPads borrowed from school remain the property of the school and can be collected in or withdrawn at any time.

• When school ICT equipment is borrowed by staff it should be signed out with the Headteacher in the Loans Book.

• The ICT Technician provided by external company CMAT is responsible for ensuring staff have access to the latest anti-virus software, as recommended by the LA, and that there is opportunity for this to be installed on all laptops/ tablets.

• It is the responsibility of all staff with a laptop, to ensure that once anti- virus software is installed, it is kept up to date; this is done by connecting to the school network on a regular basis so that updates can be transferred from the server to the laptop.

• Staff laptops/iPads can be used for personal use i.e. Internet banking/shopping, legal downloads etc. ***However – it is the responsibility of staff to ensure that the sites they use are safe and will not cause any damage to the school network***. Personal use of school hardware should only occur outside the normal hours of the school day.

• School ICT equipment must not be used for personal interests of an unacceptable or illegal nature.

• If school ICT equipment is used by persons other than those employed by the school, (i.e. partners and pupils) it is the responsibility of staff to ensure that the device is being used in accordance with these ICT Acceptable Use guidelines.

Viruses could cause serious harm to the school network, and this could result in not only the loss of large amounts of pupils and staff work, but could also result in severe damage to all the hardware. Therefore, if a virus from a staff laptop is transferred onto the school network, this will be dealt with as a serious matter.

Disciplinary Procedures

Any member of staff who misuses the school's ICT facilities and fails to follow the ICT Acceptable Use Policy will be barred from using any such ICT facilities and may be subject to disciplinary procedures.

Any student, volunteer worker, parent/carer or community user who misuses the school's computer facilities and fails to follow the ICT Acceptable Use Policy will be barred from using any such ICT facilities and, depending upon the nature of the misuse, the police would be involved.

Last reviewed: 1.9.2
Date of next review: on or before 1.9.25