
Croughton All Saints CE Primary School

Acceptable Use Policy

September 2023



Be Ready, Be Respectful, Be Safe – To believe, achieve, succeed together’.

This is firmly rooted in Christian values. We look to Jesus as our guiding light. He inspires us to live out our Christian values and strive for excellence in all we do; celebrating life in all its fullness. Jesus said 'I have come that you may have life in all its fullness' (John 10:10). He calls us to a full life in mind, body, heart and spirit.

Reviewed by	Approved by	Date Approved	Next Review Date
S.Smith Headteacher L.Davis STEM leader	FGB	October 2023	October 2024

Introduction

This policy is designed to enable acceptable use for all staff and governors. Croughton All Saints C OF E Primary School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of both staff, governors and pupils, it is important that all staff members and governors follow the guidelines detailed below.

This Acceptable Use Policy aims to:

- Promote the professional, ethical, lawful and productive use of the School's ICT systems.
- Define and identify unacceptable use of the school's ICT systems and external systems.
- Educate all users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and school devices.
- Specify the consequences of non-compliance.

This policy applies to staff members and governors, and all users of the School's ICT systems are expected to read and understand this policy. Breach of this policy may result in disciplinary action. The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018. If you are in doubt and require clarification on any part of this document, please speak to the School Business Manager or Headteacher.

Contents

Introduction	1
Provision of ICT Systems	2
Network Access and Security	2
School Email.....	3
Internet Access.....	4
Digital Cameras	5
File Storage	5
Mobile Phones	5
Social networking.....	6
Sharing of Media.....	6
Children’s School Accounts.....	6
Monitoring of the ICT Systems	7

Provision of ICT Systems

- All equipment that constitutes the School’s ICT systems is the sole property of the School. No personal equipment should be connected to or used with the School’s ICT systems. This list includes but is not extensive to:
 - laptops
 - iPads
 - computers
 - tablets
 - school phones
 - digital cameras
 - printers
- Users must not try to install any software on the ICT systems without permission from the Head teacher or Computing lead.
- If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.
- Individual laptop/desktop computers or any other ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason.
- Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.
- Users are not permitted to make any physical alteration, either internally or externally, to the School’s computer and network hardware.
- If a user has any issues with a laptop or device, this should be reported to the Computing Lead or Headteacher as soon as possible to rectify or provisionally replace if necessary.

Network Access and Security

- All users of the ICT systems at the School must first be registered.
- Following registration, a network user account will be created, consisting of a username, password and an e-mail address.
- All passwords should be complex to ensure data and network security.
- All user account details are for the exclusive use of the individual to whom they are allocated.
- Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.
- All users are personally responsible and accountable for all activities carried out under their user account(s).
- Users must ensure devices are not left unprotected and are password secured at all times when not in use.
- Users are permitted to take home any devices but it is their sole responsibility and any damages could incur a fee.
- Users must take all reasonable precautions to protect their user account details and must not share them to any other person, except to the Headteacher, Computing Lead or School Business Manager for the purposes of system support.
- Users must report any security breach or suspected breach of their network, email or application account credentials to the Headteacher, Computing Lead or School Business Manager as soon as possible.
- Users should only access areas of the schools' computer systems to which they have authorised access.
- When any device such as a laptop or computer is left unattended, it must either be logged off or locked as a safety precaution. It is the responsibility of the user to ensure this.
- Activity that threatens the integrity of the school ICT systems, or activity which attacks or corrupts other systems, is forbidden.
- Users' internet activity must not compromise the security of the data on the school ICT systems or cause difficulties for any other users.
- Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.

School Email

Where an email is provided, it is for academic and professional use, with reasonable personal use being permitted. Personal use should be limited to short periods during recognised break times and comply with this acceptable use policy. The School's email system can be accessed from both the school computers, and via the internet from any computer. All school related communication must be via the school email address. The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted. Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email or password protection.

- Emails should never contain children's full names either in the subject line or preferably not in the main body of the text. Initials should be used wherever possible.
- Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded.
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Staff are given a grace period of time of 24 'working' hours to respond to any email queries.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media account.

Internet Access

Internet access is provided for academic and professional use, with reasonable personal use being permitted. Priority must always be given to academic and professional use. The School's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to the Computing lead or Headteacher. Staff must not therefore access from the School's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral. Misuse of the internet may, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading the following material, or using the following facilities, will amount to gross misconduct (list is not exhaustive):

- accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials
- transmitting a false and/or defamatory statement about any person or organisation
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others
- transmitting confidential information about the School, staff, students or associated third parties
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School)
- downloading or disseminating material in breach of copyright
- engaging in online chat rooms, instant messaging, social networking sites and online gambling
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child

Any such action will be treated very seriously and may result in disciplinary action. Where evidence of misuse is found the School may undertake a more detailed investigation, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure. If necessary such information may be handed to the police in connection with a criminal investigation.

Digital Cameras

The school encourages the use of digital cameras and video equipment; however, all staff should be aware of the following guidelines:

- Photographs should only be named with the pupil's name if they are to be accessible in school only.
- All class teachers have been provided with a digital camera. It is the sole responsibility of each teacher to keep these safe and use them where appropriate.
- All photographs or videos taken should be uploaded to the school One Drive network.
- No full names of children should be published on the school website when being linked with a photograph.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones or iPads.
- All photos should be downloaded to the school network by the class teachers or teaching assistants regularly.
- The use of mobile phones for taking photos of pupils is not permitted anywhere on the school grounds by staff, governors or third-party groups.

File Storage

- Staff members have their own personal area on the network, as well as access to shared network drives such as the communal One Drive.
- Any school related work should be stored on the school One Drive network and this should be kept up to date daily to ensure full access.
- Personal files are not permitted on the network areas.
- Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files.
- The storing of any files on removable media, such as USB drives or a personal computer, is not permitted.
- No school data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

Mobile Phones

Mobile phones are permitted in school, with the following restrictions:

- Mobile phones are not to be used when members of staff are directly supervising or working with children.
- Whilst members of staff are working in the classroom, mobile phones should be securely stored in a bag within a locker and not in the same room.
- Personal mobile phone cameras are not to be used on school trips.
- The school has provided digital cameras to all class teachers for this purpose.
- All phone contact with parents regarding school issues will be through the school's phones.
- Personal mobile numbers should not be given to parents at the school.
- Mobile phone use is permitted in the staffroom during the school day.
- Mobile phone use is permitted outside of contact time which is from 8:40am-3:15pm, unless a club is also running.
- Staff are expected to be sensible when using their phones outside of these times as there may still be children present on the school grounds in some cases due to clubs.

Social networking

The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the school, staff and students at all times and that they treat colleagues, students and associates of the school with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the school's reputation, nor the reputation of individuals within the school are compromised by inappropriate postings.
- Use of social networking sites for school business is not permitted, unless via an officially recognised school site and with the permission of the Headteacher.
- Members of staff will notify the Headteacher if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos, which show pupils of the school who are not directly related to the person posting them, should be uploaded to any site other than the school's Website.
- No comment, images or other material may be posted anywhere, by any method that may bring the school or, the profession into disrepute.
- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook).
- The school will use social media to share information with parents where it is necessary or to promote an event happening, and this is at the discretion of the headteacher.

Sharing of Media

In some cases, photographs and videos may be shared with parents and carers. This must always be at the decision of the Headteacher. Any media must be shared via a secure sharing system. The school is currently using the WeTransfer website at the suggestion of the Computing Lead, which ensures only those with the connected link can access the media sent across. Within one week this media deletes itself and the link becomes void. This link is sent directly from the School Business Manager to the parents email addresses, and is only sent once the parents or carers have confirmed they are happy for the media to be shared.

Children's School Accounts

Throughout children's time at Croughton All Saints C OF E Primary School, they will need to have digital accounts made for them to access different parts of their learning. These accounts will be created with a username and password which the class teacher will have access to and can share readily with the children if they need them. These accounts will not

use the children's full names as a user name, but may use the following, E.G. John Smith could be Smith10, or in the case of Edshed a made-up alias is used This list is not exhaustive to, but covers accounts such as:

- Edshed and Mathshed for spellings and homework (this is shared with parents)
- Renaissance for reading quizzes and assessments
- A Windows computer login
- Scratch (ICT Computing software)
- TinkerCAD (ICT Computing software)

Children will have access to computing software including laptops, computers and iPads during their day which will be used in different lessons for research, building and learning. Before using any device, children should be reminded of the child friendly 'Acceptable Use Policy' which will be displayed in their classrooms and on the storage for such devices.

Monitoring of the ICT Systems

The school may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the school's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by the Headteacher to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided
- maintain the systems
- prevent a breach of the law, this policy, or any other school policy
- investigate a suspected breach of the law, this policy, or any other school policy.

Failure to Comply with the Policy Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal. Any unauthorised use of the school's ICT systems, One Drive network, ICT systems, the internet, e-mail and/or social networking site accounts, which the Headteacher considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority. The school reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.