



Acceptable Use Policy



Introduction

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. As part of **The Federation of Skelton Newby Hall CE Primary and Sharow CE Primary School's** programme to comply with the new legislation it has written a new suite of Information Governance policies.

The Acceptable Use policy governs the use of the School's corporate network that individuals use on a daily basis in order to carry out business functions.

This agreement is designed to ensure that all members of staff are aware of their professional responsibilities when using any form of technology. Technology relates to ICT systems, hardware, software, internet, email, Learning Platforms, web2 technologies, mobile devices, cameras, laptops and memory devices.

This policy should be read in conjunction with the other policies in the School's Information Governance policy framework.

Scope

All policies in **The Federation of Skelton Newby Hall CE Primary and Sharow CE Primary School's** Information Governance policy framework apply to all School employees, any authorised agents working on behalf of the School, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

Email and Instant Messaging Use

The School provides email accounts to employees to assist with performance of their duties. The School also allows employees to use its instant messaging service. For the benefit of doubt Instant Messages are classed as email communications in this policy.

Personal Use

Whilst email accounts should primarily be used for business functions, incidental and occasional use of the email account in a personal capacity may be permitted so long as:

- Personal messages do not tarnish the reputation of the School,
- Employees understand that emails sent to and from corporate accounts are the property of the School,
- Employees understand that School management may have access to their email account and any personal messages contained within,
- Employees understand that the Emails sent to/from their email account may have to be disclosed under Freedom of Information and/or Data Protection legislation,
- Employees understand that the School reserves the right to cleanse email accounts at regular intervals which could result in personal emails being erased from the corporate network,
- Use of corporate email accounts for personal use does not infringe on business functions.

Inappropriate Use

The School does not permit individuals to send, forward, or solicit emails that in any way may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit messages, images, cartoons, jokes or movie files,
- Unwelcome propositions,
- Profanity, obscenity, slander, or libel,
- Ethnic, religious, or racial slurs,
- Political beliefs or commentary,
- Any messages that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Other Business Use

Users are not permitted to use emails to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School management.

Email Security

Users will take care to use their email accounts in accordance with the School's information security policy. In particular users will:

- Not click on links in emails from un-trusted or unverified sources,
- Use secure email transmission methods when sending personal data,
- Not sign up to marketing material that could jeopardise the School's IT network,
- Not send excessively large email attachments without authorisation from School management and the School's IT provider.

Group Email Accounts

Individuals may also be permitted access to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to suspension of an individual's email rights. The Headteacher will have overall responsibility for allowing access to group email accounts but this responsibility may be devolved to other individuals.

The School may monitor and review all email traffic that comes to and from individual and group email accounts.

Internet Use

The School provides internet access to employees to assist with performance of their duties.

Personal Use

Whilst the internet should primarily be used for business functions, incidental and occasional use of the internet in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the School,
- Employees understand that School management may have access to their internet browsers and browsing history contained within,
- Employees understand that the School reserves the right to suspend internet access at any time,
- Use of the internet for personal use does not infringe on business functions.

Inappropriate Use

The School does not permit individuals use the internet in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic images, cartoons, jokes or movie files,
- Images, cartoons, jokes or movie files containing ethnic, religious, or racial slurs,
- Any content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Individuals are also not permitted to use the internet in a way which could affect usage for others. This means not streaming or downloading media files and not using the internet for playing online games.

Other Business Use

Users are not permitted to use the internet to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School management.

Internet Security

Users will take care to use the internet in accordance with the School's information security policy. In particular users will not click on links on un-trusted or unverified WebPages.

Social Media Use

The School recognises and embraces the benefits and opportunities that social media can contribute to an organisation. The School also recognises that the use of social media is a data protection risk due to its open nature and capacity to broadcast to a large amount of people in a short amount of time.

Corporate Accounts

The School has a number of social media accounts across multiple platforms. Nominated employees will have access to these accounts and are permitted to post general information about the School. Authorised employees will be given the usernames and passwords to these accounts which must not be disclosed to any other individual within or external to the organisation.

The Headteacher will have overall responsibility for allowing access to social media accounts.

Corporate Social Media Accounts must not be used for the dissemination of personal data either in an open forum or by direct message. This would be a contravention of the School's information governance policies and data protection legislation.

Corporate Social Media Accounts must not be used in a way which could:

- Tarnish the reputation of the School,
- Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.
- Be construed as sexually explicit,
- Construed as political beliefs or commentary.

Personal Accounts

The School understands that many employees will use or have access to Personal Social Media Accounts. Employees must not use these accounts:

- During working hours,
- Using corporate equipment,

- To conduct corporate business,
- To contact or approach clients, customers, or partners of the School.

Telephone and Skype Use

The School provides email accounts to employees to assist with performance of their duties. The School also allows employees to use Skype for Business. For the benefit of doubt Skype calls are classed as telephone calls in this policy.

Personal Use

Whilst the telephone should primarily be used for business functions, incidental and occasional use of the telephone in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the School,
- Employees understand that School management may have access to call history,
- Employees understand that the School reserves the right to suspend telephone usage at any time,
- Use of the telephone for personal use does not infringe on business functions.

Inappropriate Use

The School does not permit individuals use the telephone in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

Other Business Use

Users are not permitted to use the telephone to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School management.

General information

- User have a duty to protect their passwords and personal network and logins, and should log off the network when leaving a workstation unattended.
- Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- Have a duty to protect their passwords and personal network and Learning Platform logins, and should log off the network and Learning Platform when leaving a workstation unattended. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- Must not install any software or hardware without permission from a technician or the ICT coordinator.
- Are not permitted to use personal portable media for storage of school related data/images (e.g. USB stick) without the express permission of the Headteacher.

- Should ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off school premises, or accessed remotely. Personal data can only be taken out of school when authorised by the Headteacher or Governing Body.
- Are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, including when on external trips/visits. With the written consent of parents (on behalf of parents) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. Digital images are easy to capture, reproduce and publish and, therefore, misused.
- Should ensure that their use of web 2 technologies, including social networking sites, such as Facebook, Bebo, and Myspace, does not question or bring their professional role into disrepute. Members of staff: are advised to consider, and set appropriately, their privacy settings on such sites.
- Should consider the appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
- Should not communicate with pupils, in relation to either school or non school business, via web 2 technologies. Members of staff should only communicate with pupils using the appropriate LA/school learning platforms or other systems approved by the Headteacher.
- Are not permitted to contact or communicate with pupils, parents or conduct school business using personal email addresses or telephones, without specific permission from the Headteacher.
- Should not give out their own personal details, such as telephone/mobile number or email address, to pupils.
- Must ensure that all electronic communication with pupils and staff is compatible with their professional role.
- Must promote and model positive use of current and new technologies and e-safety. Members of staff can access information about e-safety from the North Yorkshire Primary ICT room and within the North Yorkshire Learning Platform and from the Learning Network. The e-safety coordinator can also provide information, resources and guidance.
- Must respect and comply with copyright and intellectual property rights.
- Have a responsibility to report any misuses of technology, including the unacceptable conduct of others, to the e-safety coordinator or Headteacher.

User Signature

I agree to follow this user agreement, and understand that failure to do so may result in disciplinary proceedings in line with the School's Disciplinary Procedure.

Signature **Date**

Full Name **Job Title**
(Printed)