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 West Heslerton C.E. 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 policy should be read in conjunction with the other policies in the School's Information Governance policy framework.

Scope

All policies in West Heslerton C.E. 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,
- Use of and information stored on all 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 and Dojo access to employees to assist with performance of their duties.

Personal Use

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

- Personal messages do not tarnish the reputation of the School,
- Employees understand that messages sent to and from corporate accounts are the property of the School,
- Employees understand that School management may have access to their accounts and any personal messages contained within,

- Employees understand that the emails and messages sent to/from their accounts may have to be disclosed under Freedom of Information and/or Data Protection legislation,
- Employees understand that the School reserves the right to cleanse accounts at regular intervals which could result in personal emails being erased from the corporate network,
- Use of corporate 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 and messaging 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.

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

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

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

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

Use of Devices

All devices on the premises which have cameras, videos or internet access are used appropriately.
Staff must use school equipment for taking images.

Images are printed or reproduced at the setting to ensure that photos or recordings cannot be used inappropriately.
School equipment is not taken off the premises beyond school hours unless by prior arrangement eg trips, staff working at home.
Personal devices are stored away from classrooms in a secure area and used away from pupils during breaks during the schools.

Internet Use

The School provides internet access to employees to assist with performance of their duties. All internet access is filtered and use is monitored through Smoothwall.

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 sites.

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.

School 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.

School 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.

School 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 Video Calls

The School provides email accounts to employees to assist with performance of their duties. The School also allows employees to use Video conferencing. For the benefit of doubt these 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 to 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.

Telephone Conduct.
All members of staff are expected to answer the phone when necessary in a professional manner. Messages should be recorded in the telephone message book and brought to the attention of the relevant member of staff at the earliest opportunity.
Personal phone calls are permitted with the permission of the most senior member of staff available.

Date of review: Summer 2025
Date of next review: Summer 2028 (unless required sooner)