Information Technology Acceptable Use Policy

West Heath School

WESTHEATH

REBUILDING LIVES THROUGH EDUCATION

Approved by:	Board of Trustees	**Date:** March 2023	
Creation date/ Version Date:	March 2023		
Last reviewed on:	March 2023		
Next review due by:	March 2025		
Lead Persons	Online Safety Officer and Network Manager		
Policy Audience:	Staff/Volunteers/Trustees/Contractors/Parents/Students		

Contents

Copies of this policy are available on the School Website - http://www.westheathschool.com/policies-and-procedures or as a hard copy on request from the School Office.

1. Aims

This policy aims to: provide straightforward and concise guidance to staff relating to the acceptable use of computers in the school in order that the aims and objectives of the Online Safety and Data Protection policies are met.

The objectives to meet the above aims are to provide in summary requirements in relation to:

- The Internet
- The sending and receiving of emails
- Flash Drives and general use

2. Legislation and guidance

Relevant statutory guidance, circulars, legislation and other sources of information are:

- Online Safety Policy Guidance for Education Settings
- https://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety

3. Definitions

Acceptable Use is defined as use which is a legitimate and necessary part of a member of staff's professional responsibilities and activities on behalf of the School. Any use that falls outside this category is deemed to be **Personal Use**.

4. Rationale and Purpose of this Policy

West Heath School, undertakes to provide a safe environment in which all staff and students can use information technology safely and without deliberate or accidental exposure to harmful material.

It also undertakes to provide protection from malicious attacks or compromise to its systems which might result in the loss of data, corruption of data or access of sensitive information to those not entitled to it.

This policy is a summary of the key messages of the Online Safety policy and the Data Protection Policy. It gives users clear understanding of what they **can** and **can't** do, how their use will be **monitored** and **sanctions** for misuse. This policy is associated with specific training and each member of staff will be required to sign to say that they have received and understood that training.

5. Introduction

The following charts summarise the key action points from the Online Safety policy and the Data Protection policy. Staff should note that the consequences of not implementing this code are potentially very serious and a failure to do so could result in disciplinary action. The key principle behind acceptable use is enshrined in the definition of that term which centres on professional responsibilities and activities. In most cases a consideration of the definition will bring clarification. This policy will be included as part of the induction process for new staff.

6. The Internet

	It is acceptable and allowable to	It is unacceptable and forbidden to
Use	Use the internet as a resource for your professional role as a member of staff within the school. Note student searches should be made on the separate classroom network.	Use the staff network for personal and non-school related searches.
Downloading copyright materials		To download and store any copyright material e.g. movies and songs unless these are purchased by the school. In such cases the school will be the legal owner of such material.
Installing software		Install any software to any school computer. This includes add-ons and ActiveX controls needed by some web sites to run correctly. Such add-ons may only be installed by the Network Manger.
Streaming	Stream media for educational purposes and taught sessions	Use the staff network for streaming media such as watching catch-up TV, listening to the radio or news etc~~.~~
Excluded uses		Use the network for financial gain, gambling, political purpose or advertising.
You should be aware that		
All use of the internet is monitored by the school or a third party acting on behalf of the school.		
The above monitoring includes the capturing of logons and passwords.		
Misuse may result in disciplinary action.		

7. Emails

	It is acceptable and allowable to	It is unacceptable and forbidden to
Email addresses	Send and receive e-mails from a school e-mail address such as name@westheathschool.com name@westheath.org	Send or receive emails from personal e-mail accounts such as hotmail, yahoo or personal domains.
Use	Use the school e-mail addresses for school use only.	Use your school email address for personal use.
Images and attachments	Attach or embed work related documents	Receive or send any e-mails containing crude jokes, non-work related images including attachments.

You should be aware that
All emails are monitored by the school or a third party acting on behalf of the school. In the event that there is something questionable in an e-mail, you and your sender will be sent a message to say that its content is being subjected to scrutiny. If you open something which you think is a virus, alert the network team immediately. Do not close it down and presume it's gone away.
Misuse may result in disciplinary action.
You should not
Open any emails or attachments unless they are from someone you know or are expected. If you are in any doubt you should refer to the Network Manager.

8. General Issues including the Use of Flash Drives

	It is acceptable and allowable to	**It is unacceptable and forbidden to**
Flash Drives	Use a school issues flash drive to transfer files. You are advised that in order to avoid corruption of data you should only remove such devices using the "safely remove button" to the bottom right of your screen.	Use a flash drive with an alternative browser (such as Mozilla Firefox) to bypass the School's security systems
	Student sensitive or confidential data should be carried on encrypted flash drives only	Use a flash drive to install software.
		Change the screen settings.
You should be aware that		
The Network security system will recognise attempts to use flash drives to bypass the school's protection and take measures that deactivate such devices.		
At times of heavy use the network will inevitably run more slowly. At such times multiple mouse clicking is unnecessary and unhelpful. Indeed, this slows down the system further and increases the chances of your documents becoming corrupted.		
It is important to shut down all applications at the end of a session and to log off. If you think you may be the last person to use a computer that day, it should be shut down.		

9. Links with other policies

Online Safety Policy, Data Protection Policy

10. Consultees

Online Safety Officer and the Network Manager

Appendix 1

Postholder

Monitoring and evaluation: Head of Curriculum, DSL Responsible for Online Safety and Network Manager.

Appendix 2

Guidance note for staff on a response to personal e-mail via their school e-mail address – the appropriate response

An appropriate response is two-fold:

1. The email should be forwarded un-opened to your personal e-mail address.
2. A reply to the sender containing the following or similar wording:

“My employer’s e-safety policy does not permit me to respond to this e-mail. I have forwarded it to my personal address and will respond as soon as possible. Please use my personal e-mail address in future. This is yourname@youraddress.com. Alternatively you may leave me a voicemail message on my mobile. My number is 07nnn nnn nnn.”

Appendix 3

Guidance note on exchanging documents between School and home

It is fully recognised that staff work at home on documents relating to their professional activities and that it may be essential to transmit and receive them electronically.

In such cases staff should use their school e-mail address which can be accessed remotely. Any member of staff who is unsure about how to do this should consult the e-safety officer. Personal email addresses should not be used for this purpose.

All members of staff are reminded of the importance of having good virus protection.

Staff are able to access the school servers and their documents remotely via terminal services and Office 365. Please arrange this connectivity with your Line Manager and the Network Manager.