



## Information Technology Acceptable Use Policy for the West Heath Network

This policy has been written for...	All staff at West Heath School.
Copies of this policy may be obtained from...	<ul style="list-style-type: none"> <li>The shared area on the school's network</li> </ul>
This policy links with the following policies	Online Safety Policy, Data Protection Policy
Participants and consultees in the formulation of this policy were...	Online Safety Officer and the Network Manager
Edition, Review frequency and dates	<p>This is edition 8, released March 2023</p> <p>This policy will be reviewed every two years</p> <p>It is due for review in March 2025</p>
Relevant statutory guidance, circulars, legislation & other sources of information are...	<ul style="list-style-type: none"> <li><b>Online Safety Policy Guidance for Education Settings</b></li> <li><a href="https://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety">https://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety</a></li> </ul>
The Lead Member of staff is	Network Manager & Head of Curriculum
Definitions and key terms used in this policy...	<p><b>Acceptable Use</b> 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 <b>Personal Use</b>.</p>
The Rationale and Purpose of this policy	<p>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.</p> <p>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.</p> <p>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 <b>can</b> and <b>can't</b> do, how their use will be <b>monitored</b> and <b>sanctions</b> 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.</p>
Appendices	<p>Appendix 1: Names of relevant current post holders</p> <p>Appendix 2: Guidance note for staff on a response to personal e-mails</p> <p>Appendix 3: Guidance note on exchanging documents between School and home</p>

## 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.

## The Aim of this policy

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

To provide in summary form requirements in relation to:

- The Internet
- The sending and receiving of e mails
- Flash Drives and general use

## 1. The Internet

	It is acceptable and allowable to	It is unacceptable and forbidden to
<b>Use</b>	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.
<b>Downloading copyright materials</b>		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.
<b>Installing software</b>		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.
<b>Streaming</b>	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.
<b>Excluded uses</b>		Use the network for financial gain, gambling, political purpose or advertising.
<b>You should be aware that</b>		
<b>All use of the internet is monitored by the school or a third party acting on behalf of the school.</b>		
<b>The above monitoring includes the capturing of logons and passwords.</b>		
<b>Misuse may result in disciplinary action.</b>		

## 2. E mails

	It is acceptable and allowable to	It is unacceptable and forbidden to
<b>E mail addresses</b>	Send and receive e-mails from a school e-mail address such as name@westheathschool.com name@westheath.org	Send or receive e-mails from personal e-mail accounts such as hotmail, yahoo or personal domains.
<b>Use</b>	Use the school e-mail addresses for school use only.	Use your school e-mail address for personal use.
<b>Images and attachments</b>	Attach or embed work related documents	Receive or send any e-mails containing crude jokes, non work-related images including attachments.
<b>You should be aware that</b>		
All e-mails 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.		
<b>You should not</b>		
<b>Open any e mails 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.</b>		

## 3. General Issues including the Use of Flash Drives

	It is acceptable and allowable to	It is unacceptable and forbidden to
<b>Flash Drives</b>	Use a school issues flash drive to transfer files. You 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 by-pass 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.
<b>You should be aware that</b>		
The Network security system will recognise attempts to use flash drives to by pass 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.		
<b>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.</b>		

### Monitoring & Evaluation

Head of Curriculum  
Network Manager  
Governance

## Appendix 1

### Post Holders

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

## Appendix 2

### Guidance Note: If a member of staff receives a 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](mailto:yourname@youraddress.com). Alternatively you may leave me a voicemail message on my mobile. My number is 07nnn nnn nnn.”

## Appendix 3

### Guidance Note: 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 e-mail 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