West Heath School
Ashgrove Road Sevenoaks TN13 1SR
www.westheathschool.com

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…	• The School **web site -** http://www.westheathschool.com • It is available as a hard copy on request from the **school office**. • Hard copies for reference are filed in the **staff room**
This policy links with the following policies	All the documents described in the Summary chart of ICT Policies most notably the 2 overarching policies - Online Safety Policy, Security & Data Management policy. The Data Protection Policy.
Participants and consultees in the formulation of this policy were…	The School's e-safety officer, the network manager, an independent e-safely advisor, parent consultation group.
Edition, Review frequency and dates	This is edition 6, released June 2017 This policy will be reviewed annually. It is due for review in June 2018
Relevant statutory guidance, circulars, legislation & other sources of information are…	• **Online Safety Policy Guidance for Education Settings** • http://www.kelsi.org.uk/__data/assets/pdf_file/0019/61642/Online-Safety-Policy-Guidance-September-2016.pdf (accessed 20th April 2017)
The Lead Member of staff is	Network Manager & Head of Residential Care and Safeguarding
Definitions and key terms used in this policy…	**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.**
The 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 Security and Data Management 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.
Appendices	Appendix 1: Names of relevant current post holders Appendix 2: Guidance note for staff on a response to personal e-mails Appendix 3: Guidance note on exchanging documents between School and home Appendix 4: Social networking

	Introduction	The following charts summarise the key action points from the Online Safety policy and the Security and Data Management 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 two parent policies (Internet (e-safety) policy, security & Data Management policy) 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
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.		

2. E mails

	It is acceptable and allowable to	It is unacceptable and forbidden to
E mail addresses	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.
Use	Use the school e-mail addresses for school use only.	Use your school e-mail address for personal use.
Images and attachments	Attach or embed work related images	Receive or send any e-mails containing crude jokes, non work related images including attachments.

You should be aware that
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.
Misuse may result in disciplinary action.

You should not
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.

3. General Issues including the Use of Flash Drives

	It is acceptable and allowable to	It is unacceptable and forbidden to
Flash Drives	Use a 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.

You should be aware that
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.
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.

Monitoring & Evaluation	Vice Principal Commissioning and Development Health & Safety Committee

Appendix 1

Post Holders

Monitoring and evaluation: Vice Principal for Commissioning and Development Julian Roberts
The current e-safety officer is Julie Goodyear - Head of Residential Care and Safeguarding
The current network manager is Marc Wenham
The person responsible for e-training is Helen Perridge – CIS 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*. 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. Please arrange this connectivity with your line manager and the Network Manager

Appendix 4

Memo to all staff from the Principal 4th March 2009: Social Networking

Staff are not permitted to communicate with students using Social Networking Sites (e.g. Facebook or Bebo), IM (Instant Messaging e.g. MSN) or Online Gaming (e.g. Xbox Live).

Extract from the Ethics Policy included in this memo

The reputation of our school is vital to our work and as such must be earned, safeguarded and cherished. Years of developing and maintaining a good reputation could be lost overnight by careless words and deeds! It is incumbent on every member of staff and anyone else working on behalf of the School whether paid or not, to take this with the utmost seriousness.

All members of staff need to be aware at all times of any actual or potential conflict of interest between the best interests of the school and its students and themselves. All relationships between staff and students should be strictly professional. Staff considering giving students their personal contact information such as mobile phone numbers should seek guidance from a senior member of staff before doing so.

Letter to all staff from the Principal (Vice principal Care at time of writing letter), 22 October 2013; Social Networking

The New School at West Heath

Ashgrove Road, Sevenoaks, Kent, TN13 ^SR

Telephone: 01732 460553

Facsimile: 01732 456734

www.westheathschool.com

Principal & Chief Executive: Christine Wells (BA Hons.)

REBUILDING LIVES THROUGH EDUCATION
at Diana, Princess of Wales'
former school

22nd October 2013

To all Staff,

After recent concerns nationally with children and adults inappropriately using social networking sites, it has highlighted the need for staff to take precautions in order to protect themselves both professionally and personally whilst using these sites.

Be very conscious of both your professional reputation and that of the setting when you are online. All members of staff are strongly advised, in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it. Staff must also be mindful that any content shared online cannot be guaranteed **to be** "private" and could potentially be seen by unintended audiences which may have consequences including civil, legal and disciplinary action being taken. Ensure your privacy settings are set appropriately. Carefully consider which settings you use (many sites have a variety of options to choose from, so make sure you understand them fully) as it could lead to your content accidentally being shared with others. Consider if you know all of your online "friends" in the real world and would you like all of their friends, who you may have never met, accessing your photos and information.

If your have a social networking account, in accordance with the school's policies **you are not permitted to have existing students or their parents/carers as 'friends' on a personal account.** It is advised not to accept ex **students or their parents/carers as "friends"** on a personal account. You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated methods. They may also be giving you access to their personal information and activities which could cause safeguarding issues and concerns. Please use your work provided email address or phone number to contact children and/or parents – this is essential in order to protect yourself as well as the wider community. If you have a pre-existing contact with a child or parent/carer outside of the school either via social networking sites or in person, you are required to inform the Principal in writing.

Be very careful when publishing any information, personal contact details, video or images etc. online; ask yourself if you would feel comfortable about a current or prospective employer, colleague, child in your care or parent/carer, viewing or sharing your content. If the answer is no, then it would probably be best not to post it online in the first place. It is also very important to be aware that sometimes content shared online, even in jest, can be misread and taken out of context which can lead to complaints and allegations being made. Staff should be aware that as professionals, we should be cautious to ensure that the content we post online does not bring the setting or our professional role into disrepute. .../2

Documents called "Cyberbullying, Supporting School Staff" and "Safer practise with Technology" are available in the staffroom to help you consider how to protect yourself online. Please photocopy them if you want or download the documents directly from www.childnet.com or www.kenttrustweb.org.uk?esafety. You can also visit Teach Today www.teachtoday.eu and the Professional Online Safety Helpline www.saferinternet.org.uk/about/helpline for more advice and information on staff safety. The Guidance for Safer Working Practice for Adults who work with Children and Young People in Education settings www.kenttrustweb.org.uk/Children/safeguards_policy.cfm is a useful piece of guidance for general matters of practice and specifically around safe practice in maintaining your professional boundaries.

I would like to remind all staff of our Acceptable Use Policy and the importance of maintaining professional boundaries online and in general. Failure to follow this guidance and the school's policies regarding online and contact in general with students, parents and carers could lead to disciplinacy action, so it is crucial that all staff understand how to protect themselves online and in their general practice.

If you have any queries or concerns regarding this letter, please speak to your designated Child Protection Co-ordinator (Jim Nunns, Alan Baker, David Porridge and Christina Wells).

Yours sincerely,
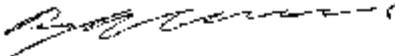
Jim Nunns
Vice Principal – Care
(On behalf of the Senior Leadership Team)