Acceptable Use Policy AUP	Name of School	Hallsville and Scott Wilkie Federation
	AUP review Date	September 2017
	Date of next Review	September 2018
	AUP Revision	11.11.09.2017
	Who reviewed this AUP?	Keri Edge – Executive Headteacher Nigel Mark – FNM Benjamin Roberts – LRM Andrea Perry – Computing Coordinator Faeeim Nori – Computing Coordinator Steve Cox – Education Consultant

Acceptable Use Policy (AUP): Staff agreement form

Covers use of all digital technologies while in school: i.e. email, internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, apps and other relevant digital systems provided by the school or school umbrella body (Local Authority, Academy, Free School Trust, etc).

Also covers school equipment when used outside of school, use of online systems provided by the school or school umbrella body when accessed from outside school, and posts on social media made from outside school premises/hours which reference the school or which might bring your professional status into disrepute.

The federation regularly reviews and updates all AUP documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may therefore be subject to monitoring.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.

- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will not engage with pupils online outside of my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (Which is currently: LGfL Staff Mail)
- I will only use the approved method/s of communicating with pupils or parents/carers: communication systems with pupils or parents/carers, and only communicate with them in a professional manner and on appropriate school business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the ICT Learning Resource Manager (LRM) or Federated Network Manager (FNM). If they are unavailable then the Computing Coordinator should be informed.
- I will not download any software or resources from the Internet that are not adequately licensed.
- I will not use any form of hacking/cracking software or system to try and bypass network or system security and obtain unauthorised access to restricted parts of the computer network, or applications contained within.
- I will not publish or distribute content that is protected by copyright. If I am unsure about the copyright status of a particular item, I will seek guidance.
- I will not connect a computer, laptop, tablet or other device to the network / Internet that does not have up-to-date anti-virus software
- I will not connect any device with removable storage such as a portable music player, mobile phone, SD Card, tablet or USB Flash/Hard Drive to the network, without first scanning it on the dedicated anti-virus scanning machines located in the staff room. I will also ensure that any removable storage devices I use are encrypted.
- If I am accompanying a visitor, who needs access to the school network, I will log them on using the highly restrictive 'visitor' account. If they have electronic resources (training materials, PowerPoint presentation etc.) I will strongly recommend that they e-mail the resources to me prior to their visit for checking. If this is not possible, visitors can bring content on a removal storage device, however, the content of the

device must be examined and the drive scanned on the dedicated anti-virus scanning machines prior to them being allowed to connect it to the network.

- I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems and I will ensure that I complete an 'ICT Equipment Agreement form' when given a new piece of equipment.
- I will return all equipment after I have finished using it / at the end of my employment and I will ensure it is left in a working and ready state for the next user. For example I will ensure laptops are shut down, and returned to the trollies, with the charging cable connected. I will also report any damaged, lost or stolen equipment to the LRM or FNM as soon as possible.
- I will not connect devices that act as a Wireless Access Point (WAP), bridge, extender, repeater or router to the network. Additionally, I will not attempt to setup any fake (honeypot) devices mimicking school hardware with the aim of trying to obtain data.
- I will not attempt to deliberately introduce a virus or malicious code to the network.
- I will not setup any device that can provide access to the Internet via a connection not provided by the school. This includes using the 'Personal Hotspot' or 'Tethering' feature available on smartphones or tablets.
- I will check the content of all videos I plan to use, to ensure they are appropriate before attempting to access them or display them in school. This includes content found on YouTube and other video sharing sites and DVDs. Only videos rated U or have been except for educational use can be displayed. All videos should be displayed in 'full screen mode' and if the video contains advertisements, these must be skipped where possible.
- I will not use personal digital cameras or any device with a camera feature, such as a mobile phone, portable games console, tablet or smartwatch for taking and transferring images of pupils or staff without permission and will not store images at home without permission. If I am accompanying a visitor who wishes to take photos, I will inform them that this is allowed, however, the following procedures must be followed:
    1. All photos must be taken on school owned equipment.
    2. All Photos will be reviewed. Photos for professional use (examples of work, pictures of the school) will be released. Photos containing children may be released, but only after it has been agreed by the parents and headteacher.
- I will take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.

- I will not use any personal device that is capable of making or receiving telephone calls (including VoIP Calls) and other communications during teaching time. I will ensure that devices are locked away during lessons. If I need to use my device, I will use it in an area that cannot be accessed by students such as the staff room.
- I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I will only access school resources remotely (such as from home) using the LGfL / school approved system (Google) and follow e-security protocols to interact with them.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the relevant Senior Member of Staff / Designated Safeguarding Lead.
- I understand that all internet and network traffic / usage can be logged and this information can be made available *to the Head* / *Safeguarding Lead* on their request.
- I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.
- *Staff that have a teaching role only:* I will embed the school's online safety / digital literacy / counter extremism curriculum into my teaching.

- I understand that failure to comply with this agreement could lead to disciplinary action.
- **User Signature**

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I agree to abide by all the points above.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature Date

Full Name (printed)

Job title

School

Authorised Signature (Head Teacher (primary) / Head/Deputy/ senior teacher (secondary))

I approve this user to be set-up.

Signature Date

Full Name (printed)