Low Ash Primary School

(Logo designed by Low Ash pupils)

Acceptable Use of ICT

and Information System

January 2017

Information and Communication Technology (ICT) Acceptable Use Policy

Rationale for Policy
As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use ICT and the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using ICT and the school systems, they are asked to read and sign this Acceptable Use Policy.
This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

Agreement
I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, digital cameras, email and social media sites.

My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking (see also social media policy), gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school Acceptable Use Policy (AUP) and the Law.

I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces

I will report all incidents of concern regarding children's online safety to the Designated Named Person (Terry Woollin, Beth Medhurst, Jane Gibson, Dan Hurst or Fiona Meer) and the e-Safety Officer (Phil Ebbage) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Officer.

I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware I will report it using the ICT fault logging system and inform the ICT Co-ordinator.

Use of School Equipment
School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 (as amended) makes attempting to gain access to other users' data and user accounts without permission a criminal offence.

I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and for educational use and appropriate personal use in their own time, outside of the school day. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my device as appropriate.

I will respect system security and I will not disclose any password or security information. I will use a 'strong' password that contains numbers, letters and symbols, with 8 or more characters.

I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager apart from the machine allocated to myself.

I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

I will not keep professional documents which contain school-related, sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones, memory sticks), unless they are <u>secured</u> and <u>encrypted</u>. I will protect the devices in my care from unapproved access or theft and ensure that they are running a suitable antivirus solution to protect infiltrating the school system.

If I have lost any school related documents or files, then I will report this to the ICT Support Provider/Co-ordinator as soon as possible using the ICT Fault Logging System.

When using any device owned by the school I will ensure that due care and attention is taken to protect it from damage, such as keeping equipment at a safe distance away from potentially damaging items such as liquids/other products. I will also ensure that care is taken when using and storing devices, both when in use and when not, for example, keeping items off the floor, or having cables in such a position that they could be a trip hazard. When transporting school equipment I understand that devices must not be left unattended e.g. in a car overnight.

If any loss or damage to school equipment does occur, either inside or outside the workplace I will report it as soon as possible to the ICT/Computing co-ordinator. Replacement of equipment if damaged when not on school premises may require individuals to assist with excess payments.

Communication with parents / carers and pupils
-I will only communicate with parents/ carers using official school systems
-I will not engage in any online activity that may compromise my professional responsibilities (see also social media policy)

Use of School Email
If another email address has been used to sign up to school related websites this must be changed to the school email address.
My use of School provided email will be related only to work purposes. I will not store any personal information on the school email system that is unrelated to school activities, such as personal photographs, files or financial information.
I will communicate with others in a professional manner. I will not use aggressive or inappropriate language

Use of Work Internet
I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person. Nor will I facilitate anything which could bring my professional role, the school, or the local authority, into disrepute.
I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Leader or the Headteacher (Child Protection Lead).

Use of Personal Devices to Access School Email
When accessing school email, I will ensure that my device is password protected, and will supervise any other user accessing my device.
I will also ensure that I do not use auto-complete forms for accessing the school email system on any machine to prevent unauthorised access.

Use of Personal Devices to Access School Internet
I understand that any device that I own and bring into school to access the internet via the school network (wired or wireless) is therefore subject to the same guidelines of use as a school device, and I accept that any internet use will be subject to both filtering and monitoring.

Clearing Storage media

I will always ensure that once I have finished using a data recording device (such as camera, video camera or Easi-Speak microphone) that I remove the content from this device and copy it to a safe designated place on the school network. I will not copy any data from any school device to a personal device as I understand that this will be a breach of our e-safety and Data Protection Policies. I also understand that if I fail to copy the data it will not be available from the device the next time I use it.

Maternity/Extended Leave
I understand that if I am away from school for any extended period of time I may have to return any school equipment to school so that it can be regularly maintained and inventoried at school, and is available for use by other members of staff as required.

Ownership of School Devices
I understand that the ownership of any device provided for my use for school is retained by school, not myself, even if I am allowed to take them home for work purposes. I also understand that any device is subject to being recalled at any time for maintenance and re-distribution if required.

Appropriate Desktop Images
I will ensure that any images displayed on my devices are suitable for the viewing of all members of the school community and should not display images of family and/or social life.

Use of Memory Sticks
I understand that external storage devices are for short term data storage only and that they do not have infinite lifespans. They are therefore unsuitable for the safe retention of any school related data. I also understand that any school data to be stored on external storage devices should be kept solely on encrypted devices, to conform with our school E-Safety and Data Protection Policies.
Any important work/data should be stored in a safe designated place on the school network, and I realise that any data lost from external storage will **not** be backed up by the school system.
I will also ensure that any external storage devices are removed from the laptop when left unattended or before transportation, either around the school, or from school to another location.

Use of Correct User Accounts
I will always use my own login account when accessing the school network.

Turning Off/Charging Equipment
I will ensure that all devices used by myself or pupils in my care will be safely shut down at the end of the day and returned to the approved secure location and set to charge where necessary.

I understand that should I not comply with any part of this policy, my action could lead to disciplinary action up to and including dismissal and/or removal of access from the School's electronic communication system.

Signed...

Staff / Volunteer name...

Date...

Policy Agreed January 2017

Signed…………………………………..
Named Person for Safeguarding/ESafety and Child Protection

Next Review January 2017

4