Staff Acceptable Use Policy for St Malachy's Catholic Primary School A Voluntary Academy 2015-16

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 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.

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, iPads, PDAs, 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, 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 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 Child Protection Co-ordinator and the e-Safety Co-ordinator Annie McNally or Alex Hudson, as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator.

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 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 only for educational use. To prevent un-authorised 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 IT system manager (Jonny Carter), including software such as i-Tunes.

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 secured and encrypted. I will protect the devices in my care from unapproved access or theft and ensure that they are running a suitable anti-virus solution to protect infiltrating the school system.

If I have lost any school related documents or files, then I will report this to the IT system manager (Jonny Carter) 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.

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 IT system manager (Jonny Carter).

Use of School E-mail

My electronic communications with pupils, parents / carers and other professionals will only take place via work approved communication channels e.g. via the school provided e-mail address or telephone number. If another email address has been used to sign up to school related websites this must be changed to the school e-mail address. My use of school provided e-mail will be related only to work purposes. I will not store any personal information on the school e-mail system that is unrelated to school activities, such as personal photographs, files or financial information.

Use of School 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 LEA 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 practice online, either in school or off site, then I will raise them with the e-Safety Coordinator or the Head Teacher.

Use of Personal Devices

I understand that staff should only use their mobile phones at appropriate times of the day e.g. break times. During the school day my mobile phone should be turned off or set to silent. I must not use my personal mobile devices or cameras to take images of pupils or staff, without prior authorisation from the e-Safety coordinator.

Use of Personal Devices to Access School E-mail

I will ensure that any device with direct access to school email systems 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 e-mail 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.

Social Media

I understand that we are now living in the age of social media, where things that are communicated often pass around the world before we've had time to think what's actually been said. Thus it has never been more important that we are all aware of what we say and write, especially on social media sites such as Facebook or Twitter.

Social media means:

- Social networking sites such as Facebook, Google+, Twitter and MySpace
- Professional networking sites such as LinkedIn
- Online chat rooms, forums and blogs
- Other social media such as Youtube and Flickr

Use of personal equipment to access social media sites, whilst you on work time

I understand that I must not use my own equipment to access social media, other than any school blog, when I am supposed to be working (i.e. regularly scheduled hours excluding meal or break periods).

Posting responsible content on social media sites

I understand that when using social media sites I am operating in a public space and my conduct may have serious consequences for the school or myself.

I will comply with the following basic rules whenever I am using social media sites.

Do:

- Remember that conversations between 'friends' on Facebook are not truly private and can still have the potential to cause damage.
- Report to the Headteacher if you see anything on a social media site that indicates that a colleague may have breached this policy.

Do not:

- Make maliciously false or harassing or discriminatory comments which violate our code of conduct policy regarding any employees or families
- Post comments or pictures containing confidential school information
- Use a school e-mail address to register on social media sites

Clearing Memory Cards

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 Absence

I understand that if I am away from school for an extended period of time I should 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 all devices 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 redistribution 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 to 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 including netbooks, laptops, PC's and Interactive Whiteboards /LCD screens

Document Updates

This document may be updated and altered. At which point it will be republished and made available to staff.

Declaration

Staff Signature _____

Staff Printed Name _____

e-Safety Coordinator Signature _____

e-Safety Coordinator Printed Name _____

Headteacher Signature _____

Headteacher Printed Name _____

Date _____