St. Patrick's R.C. Primary, Dipton

Staff ICT Acceptable Use Policy

Revision History					
Name	**Version**	**Reason for change**	**Status**	**Date**	**Review Date**
Mrs K Bevan Mrs J Burgess	1.2	Updated from Durham County Council	Final	Agreed by Standards & Curriculum Committee April 2019	April 2022
Mrs J Burgess Mrs K Bajrami	1.1	Updates	Final	Agreed by Standards and Curriculum Committee May 2018	2019
School lead: Mrs K Bajrami Reviewed by all staff Reviewed by Standards and Curriculum Committee	1.0	Review	Final	March 2016	March 2018

Introduction

This document was received from Durham County Council.
This document should be read alongside other policies in operation at St Patrick's.

This policy was originally based on guidance from Kent, and we would like to acknowledge their work.

Staff ICT Acceptable Use Policy (AUP)

Guidance for Use

In order to protect staff members, it is essential to have an AUP in place which has been viewed and understood. All employees (including teaching and non-teaching staff) must be aware of the school rules for use of information systems and professional conduct online whether on or off site. Misuse of computing systems and other professional misconduct rules for employees are specific and instances resulting in disciplinary procedures or staff dismissal have occurred.

With internet use becoming more prominent in every day life for personal and professional use, it is important that all members of staff are made aware that their online conduct both in and out of school could have an impact on their role and reputation. Civil, legal or disciplinary action could be taken should they be found to have brought the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities. It is therefore important that the AUP is firmly embedded within the school induction process for all members of staff (including any volunteers, part-time staff or work experience placements). It is also important that all members of staff receive up-to-date and relevant training around this issue on a regular basis. All members of staff should read, understand and sign the AUP before being granted access to any of the schools systems.

Some settings may wish to provide more explicit guidance for staff around use of social networking and email as, even when use of social media sites such as Facebook and Twitter occur in their own time using their own computer, it can leave staff vulnerable to abuse or a blurring of professional boundaries. Schools must be aware they cannot ban staff from using sites in their own personal time; however they can put in place appropriate guidance and boundaries around staff interaction with pupils (past or present) and parents. It is recommended that any contact with pupils and parents only takes place via school approved communication channels e.g. school email address or the school learning platform so it can be monitored and traced in the case of an allegation or concern. However, schools must recognise that in some cases there may be pre-existing relationships which mean that any "ban" from adding pupils or parents as friends or contacts on personal social networking sites may be difficult to enforce. It is therefore recommended that members of staff are encouraged to make SLT aware of these exceptions in order to protect themselves from allegations or misinterpreted situations. It is crucial that all members of staff are made aware of the boundaries and professional practices online in order to protect their professional status. Staff should be advised to check their privacy settings on any personal social media sites they use, however they should always remember that once content is shared online it is possible for it be circulated more widely than intended without consent or knowledge (even if content is though to have been deleted or privately shared).

Staff ICT Acceptable Use 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 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 Information Communication Technology 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.

1) 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, tablets, digital cameras, email and social media sites**.**

2) School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3) Mobile Phones

   a) Staff mobile phones will be stored in personal bags (until lockers are purchased) during the school day and may only be used when children are not present

   b) Cameras on personal phones or tablets will not be used to take pictures of children in any circumstances.

4) I understand that any hardware and software provided by my school for staff use can only be used by members of staff and can only be used for school related work. The children's Ipads *should not* leave the premises, each class is assigned an Ipad to be used on an educational visit. These should be password protected and the password logged with the business manager to allow continued access in the event of change of staffing.

5) Personal use of school ICT systems and connectivity is not permitted.

6) To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

7) I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 10 or more characters, does not contain a dictionary word and is only used on one system).

8) I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

9) Data Protection

   a) I will ensure that any personal data is kept in accordance with the General Data Protection Regulations. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.

   b) If I choose to use a portable device (Phone, Tablet etc…) to collect my work e-mail I will ensure that the device is locked by a pin code or password and will be wiped when I dispose of the device.

c) I will not transfer sensitive personal information from my school e-mail account (e.g. EHCP's Safeguarding Reports, Medical Information) UNLESS the information is encrypted.

d) I will not keep professional documents which contain school-related personal information (including images, files, videos etc.) on any personally owned devices (such as laptops, digital cameras, mobile phones). The use of USB drives is strictly forbidden.

e) Digital Images or videos of pupils will not be taken away from the school premises.

f) I will not use unapproved cloud storage systems (Dropbox, icloud etc) for storing personal data of staff or pupils.

10) 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.

11) I will respect copyright and intellectual property rights.

12) Social Media.

a) 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.

b) I will not communicate with pupils or ex-pupils using social media without the express permission of the Headteacher.

c) My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team. *This would include any relatives of current pupils that are my "friends" on a social media site.* It is ***strongly recommended*** that staff are not friends with parents on any social media. Facebook or other social media sites ***must not*** be used to discuss school matters with parents/'friends'. The Teacher's Standards document (2013) states that a teacher's conduct should *"at all times observe(ing) proper boundaries appropriate to a teacher's professional position".*

d) 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.

e) 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, or anything which could bring my professional role, the school, or the County Council, into disrepute. This would include any comment made, even in the belief that it is private on social media.

13) I will report all incidents of concern regarding children's online safety to the Designated Safeguarding lead (DSL) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the DSL or the designated lead for filtering as soon as possible.

14) 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 or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team at BITS.

15) I will promote Online 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.

16) 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 DSL or their deputy.

17) I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: …….... Print Name: …… Date: ……

Accepted by: …….. Print Name: ……..