Acceptable ICT Use Policy & Agreement & Social Media Policy

Staff and Governors

Committee Responsible – SLT
Last review: 2016/2017
Next Review: 2018/2019

Acceptable Use Agreement: Staff and Governors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that everyone working within the school is aware of their professional responsibilities when using any form of ICT.

Additionally the Acceptable Use Policy is there to assist the staff in staying safe and to protect the security and integrity of the school's ICT systems.

All staff and governors using ICT within school are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with St Peters E-safety coordinator or Network Manager as appropriate. Use of the school's systems outside of school is also covered by this agreement.

- I understand that ICT includes a wide range of systems and that ICT use may include personal devices when used in any professional context. I understand that any personal equipment brought into school remains my sole responsibility.

- I will only use the school's ICT for professional purposes or for uses deemed appropriate by the Head or Governing Body.

- I will comply with the ICT system security and not disclose any passwords required by any of the programmes or systems that I use. If I have any reason to believe that a password has been compromised I will immediately change it or if this is not possible ask for a new one to be issued.

- I understand that I am responsible for all activity carried out under my username and that my usage will be monitored and logged. Such logs will be available on request to SLT or the Headteacher and may be shared with the appropriate authorities if illegal activity is indicated or suspected.

- I will ensure that all electronic communications with students and staff are compatible with my professional role and such communications with students will only take place via a school email address or appropriate software. Personal accounts should not be used to communicate with students or parents / guardians.

- I will only use the approved, secure email systems for any school business.

- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

- I will not install any hardware or software without the permission of the Network Manager to ensure that the addition will not have an adverse effect on any existing programmes or system performance.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images of students and/or staff will only be taken, stored and used for professional purposes in line with school policy.

- I will respect copyright and intellectual property rights.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will report any incidents or concern regarding children's safety to the Child Protection Liaison Officer or Headteacher.

- I will report any damage to, or malfunction of, any ICT equipment to the ICT department.

- I will support the school's E-safety policy and help students to be safe and responsible in their use of ICT and related technologies. I will promote E-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

Social Media Policy

If a member of staff would like to set up a Social Media account for professional purposes, than the guidelines below should be followed:

- Any Social Media used for professional purposes should use the school logo

- Only school emails should be used to set up these accounts and all usernames and passwords should be shared with the Network Manager

before the accounts go "live"

- All such accounts should be private and anyone who wishes to follow, like, share or similar, should be checked by the member of staff who owns the account
- All such accounts should only allow a specific audience to see the media, for example a school trip with a Twitter account should only allow parents and students to follow the account and all of these must be verified by the staff member
- Staff who run these accounts should not interact by following, liking, sharing or similar with other users of social media
- If relevant, staff should ensure that parents have given permission for pictures, videos and messages to be posted about their children
- Staff should be aware that once any pictures, videos and posts have been put online, even if they are deleted later, they could be shared online and this needs to be considered at all times before posting
- If these accounts are time-limited, for example they are only relevant during a school trip, then accounts should be disabled and deleted after this period
- The Network Manager will have the right to monitor these accounts at all times

Name ……..

Signature…… Date……