### e-Policy: Managing e-mail at The Tutorial Foundation

This policy should be read particularly in conjunction with the Tutorial Foundation policy “Safeguarding and Child Protection”.

Additional supporting information is given in the Appendix at the end of this document

Within The Tutorial Foundation e-Safety is regarded as of high importance, and a cornerstone of our Safeguarding responsibilities. The obligations, rules and expectations for the school, staff and students are laid out below:

**This school:**

* Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example sen@thetutorialfoundation.co.uk for communication with the wider public.
* Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
* Manages accounts effectively with up to date account details of users.
* Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
* Knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus products, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, we have technologies to filter, monitor and protect our internet access to the World Wide Web.

**Pupils:**

* Pupils are introduced to, and use e-mail as part of the ICT scheme of work.
* Pupils are taught about the safety and ‘netiquette’ of using e-mail both in school and at home i.e. they are taught:
	+ Not to give out their e-mail address unless it is someone they know and trust and is approved by their parent/carer.
	+ That an e-mail is a form of publishing where the message should be clear, short and concise.
	+ That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
	+ They must not reveal private details of themselves or others in e‑mail, such as address, telephone number, etc.
	+ To ‘*Stop and Think,* ***Before*** *They Click’* and not open attachments unless sure the source is safe.
	+ That they should think carefully before sending any attachments.
	+ Embedding adverts is not allowed.
	+ That they must immediately tell a responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature.
	+ Not to respond to malicious or threatening messages.
	+ Not to delete malicious or threatening e-mails, but to keep them as evidence of bullying.
	+ Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them.
	+ That forwarding ‘chain’ e-mail letters is not permitted.
* Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

**Staff:**

* Staff only use school e-mail systems for professional purposes.
* Access in school to external personal e-mail accounts may be blocked.
* Never use email to transfer staff or pupil personal data.
* Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school ‘house-style’:
	+ The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used.
	+ The sending of chain letters is not permitted.
	+ Embedding adverts is not allowed.
* All staff sign school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Policy Sign off and review

|  |  |  |
| --- | --- | --- |
|  | **By whom** | **Date** |
| **Policy signed off by** | Julia Low | 15.01.16 |
| **Reviewed by** | Tim Low | 30.01.2019 |
| **Next Review By** | Julia Low | 31.01.2020 |

### Appendix 1 – further information

In the school context, e‑mail should not be considered private and most schools, and indeed Councils and businesses, reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

The use of personal e-mail addresses for professional purposes, such as Hotmail, must be avoided by all staff working in schools

Email must not be used by staff to transfer information about pupils – unless it is within an encrypted, secured email system. It is worth knowing that the data (in emails or other systems) does not belong to the User but to the organisation and they are not authorised to do as they please with the organisation's data. Therefore a school user could be personally liable for breaching the Data Protection Act (DPA98) if personal information was disclosed because of their unauthorised actions.

[Email practice has direct relevance to your school Information Handling / security policy and should be considered both by the School’s Senior Information Risk Officer (SIRO) and the Information Asset Owner. Both these individuals should be named].