



This document sets out the security, administration and internal rules which staff should observe when communicating electronically or using the IT facilities provided by Harrow School (the '**School**'). Staff should familiarise themselves with the terms of this Policy in order to minimise potential difficulties for themselves, colleagues, pupils and the School, which may arise as a result of misuse of email or internet facilities.

- 1. School Systems**
 - 1.1 The School acknowledges and welcomes the creativity of staff in the production and storage of material to support teaching, learning and administration. It is important to note that, according to the letter of the law, computer files and electronic messages created and stored on school systems by employees, contractors and residents in the performance of their normal duties technically remain the property of the School. In any question regarding copyright and intellectual property, staff are encouraged to seek advice from the IT Services Department.
- 2. Monitoring**
 - 2.1 The School's computer network is a business and educational tool to be used primarily for School business or educational purposes. Staff therefore have a responsibility to use these resources in an appropriate, professional and lawful manner.
 - 2.2 All messages and files on the School's system will be treated as education or business related which may be monitored. Accordingly, staff should not expect any information or document transmitted or stored on the School's computer network to be entirely private.
 - 2.3 You should also be aware that the School maintains systems that automatically monitor and filter use of the internet, both during school or working hours and outside of those hours. This includes the sites and content visited and the length of time spent using the internet.
 - 2.4 Staff should structure electronic messages in recognition of the fact that the School may, if concerned about possible misuse, have the need to examine its contents.
 - 2.5 Data that the School holds will be archived by the School as it considers appropriate and to comply with statutory requirements.
 - 2.6 The School will routinely send out phishing test emails to staff as part of our cyber security process. Staff that routinely click on phishing emails, both genuine or test, may be subject to disciplinary action depending upon the circumstances.