To nurture each individual's aspirations and talent

To provide outstanding learning experiences and opportunities

To promote respect for one another and the environment

To encourage collaboration and partnership

E-Safety Policy

Author:	**Andy Wareham**
Date of approval:	**19th July 2013**
Next Review date:	**July 2016**
Review period:	**3 Years**
Status:	**Recommended**
	Relevant legislation:
	Malicious Communications Act (2002)
	Data Protection Act (1998)
	Computer Misuse Act (1990)

1. PURPOSE

Farmor's School is committed to providing ICT facilities (including internet, email and the school's learning platform) to employees and students and to promoting employee awareness of the benefits and dangers involved. Improper use of the internet or email could bring the school into disrepute and may lead to legal claims against individuals and the school.

Infringement of this policy by employees may be regarded as a disciplinary offence and in serious cases, may result in dismissal.

Infringement by students may result in the withdrawal of access to hardware or software and in serious cases (particularly those that break the law) students may be excluded.

2. RELATIONSHIP TO OTHER POLICIES

This policy sits alongside the ICT Acceptable Use Policy, Data Protection Policy and Safeguarding Policy.

3. SCOPE, PRINCIPLES AND DEFINITIONS

Staff and students will be expected to sign the ICT Acceptable Use Policy (AUP) at the beginning of each academic year (see versions in the appendix). These documents highlight the school's expectations and detail what is unacceptable.

The head of ICT and the Network Manager will monitor and update the guidance set out in the AUP forms.

The Network Manager will monitor the completion and return of the AUP forms.

It is the responsibility of staff and students to keep their passwords secure.

Ownership of all computer hardware, software and documents lies with the school, and the school reserves the right to monitor, log, record and access all communications at all times.

Employees and students should be aware that their use of the internet is filtered and may be subject to monitoring by South West Grid for Learning (SWGfL) to ensure compliance with the AUP.

Employees and students should be aware that their use of the email facilities is filtered by the school to ensure compliance with the AUP.

Clear reporting procedures will be publicised in areas around the school with ICT facilities. These will be checked, maintained and up-dated by the IT technicians.

The Local Authority and Safeguarding Children guidelines state that teaching staff should avoid contacting students on social networking sites (see the appendix in the Safeguarding Policy). This is to avoid any possible misinterpretation of motives and the risk of any allegations being made.

<u>Incident procedures</u>

In the case of an e-safety incident the procedures highlighted in the e-safety incident flow chart will be followed (see appendix).

4. CONSULTATION

This policy contains no significant changes to the previous version so there has been no consultation. The previous version was discussed and agreed by the Network Management Group, ICT Users' Forum, SLT, Staff, School Council and parents.

5. MONITORING, REPORTING AND EVALUATION

Adherence to this policy will be monitored by the Network Manager who will report all e-safety incidents to the member of SLT responsible for ICT in the school and the Headteacher in the case of an incident involving a member of staff.