E-Safety - Technician Acceptable Use Policy Extension

The school ICT Technician or person with administration rights is placed in an exceptional position of trust. Many of the duties that the Headteacher expects these people to complete could be against the Staff Acceptable User Policy of the school.

This document is not a job description but an addition to the Staff Acceptable User Policy that allows the ICT technician to fulfil these duties.

Areas of concern are that:

- Files may be created, imported or processed by staff and pupils and stored on the school's servers or other storage systems (e.g.USB memory sticks, SD cards etc.) that might be of an inappropriate nature to the school setting. Inappropriate use includes any production, processing or transmission of offensive, provocative, racist, unethical, irreligious or anti-social materials in any format. Also included in this area are any materials that are against the rules and conditions of service for the school e.g. material that might bring the establishment into disrepute. Work created during the school's time or on the school's equipment or on one's own equipment but for school work, belongs to the school.

- The ICT Technician requires authorisation (and associated permissions) to create, change and delete users accounts.

- Through work within the school's administration network the ICT Technician may be placed in the position of assisting in the processing of confidential information including children's health or MIS data, confidential letters or information from or to senior staff, budgeting plans etc.

- The ICT technicians through specific user names and password have control, (sometimes through remote workstations) to the schools network.

Because of these areas of concern the ICT Technician should:

- be responsible for monitoring the school's network.

- be given permission to access other user's files.

- protect the users by maintaining a filter for the school.

- monitor the internet use of users within the school.

- be aware of the laws relating to the use of computers especially those around Data Protection, Copyright and those referred to in the school's e-safety Policy and AUPs.

- make sure that they record all user names and passwords for all the services they access in a place where the senior leaders in the school can access them (a copy is currently held in the office safe).

- have their use of the school's network, internet and other aspects of their work open for scrutiny.

To enable them to discharge these duties they should:

- receive training on the sensitive nature of their job especially in relation to Data Protection and the confidentiality of information.
- have an agreed procedure for managing the internet filter. This should include a log of decisions made.
- have an agreed understanding of what is expected of them as far as the regular monitoring of the network system and internet.
- have agreed procedures for reporting incidents.
- log any incidents including minor ones that are quickly resolved.
- be careful to make sure that they are observed when investigating serious incidents to make sure that they are protected against any allegations that could arise (e.g. never open websites that are suspected of having inappropriate material unless others are present).
- have frequent meetings with their line manger to report on any issues or trends.

As an ICT Technician (or a person who has similar responsibilities) I have read the above document and understand that I will be directed by senior staff to complete work outside of the Staff Acceptable User Policy.

I will report all concerns I have to the appropriate member of Senior Management.

Name: _____

Signed: _____

Senior Member of Staff: _____

Date: _____