Acceptable IT Use Agreement – Staff

Note: All internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both, you must sign this policy sheet.

Internet Access – You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-Safety Officer (Sarah Mitchell) and an incident sheet completed.

Social Networking – is allowed in school in accordance with the e-Safety Policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks.

Use of Email – Staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the *Data Protection Act.* As the email accounts belong to the school, emails can be accessed by the Headteacher.

Passwords – All staff have personal passwords for laptops, MyConcern, etc. Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support. Shared passwords, e.g. Google Calendar, are to be changed by the Headteacher and/or the school office team only.

Remote Access – You must keep all login and password details for remote access secure, never saved or stored an any device outside school and always logout completely when the remote access session has finished. Staff must take all reasonable precautions to ensure remote access sessions are secure.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive, etc.) is encrypted. On no occasion should data concerning personal information be taken off site on an unencrypted device.

Personal Use of School IT – You are not permitted to use IT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos – You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal IT – Use of personal IT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment. A risk assessment will be carried out by IT support and the e-Safety Officer.

Viruses and Other Malware – Any virus outbreaks are to be reported to the e-Safety Officer and Headteacher as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Purchasing Apps/Software – This must be in agreement with the e-Safety Officer and computing co-ordinator to ensure validity and safety for students.

e-Safety – Like health and safety, e-safety is the responsibility of everyone to everyone. As such, you will promote positive e-safety messages in all use of IT whether you are with other members of staff or with students.

e-Safety concerns must be logged on MyConcern.

I understand that any breach of the policy may lead to disciplinary action.

NAME:

SIGNATURE: **DATE:**