Electronic Communications Acceptable Use Policy

Use of the internet by staff is permitted and encouraged where such use is suitable for school and educational purposes and supports the workings of the school. The internet is to be used in a manner that is consistent with the school's ethos and expected standards of staff conduct, and as part of the user's job description.

1.Compliance with E-Safety policy

Staff must comply with all aspects of the E-Safety policy (which must be signed), which covers:

- Roles & Responsibilities
- Teaching & Learning
- Use of electronic communications
- Administration and management
- Response to incidents of concern
- Parental involvement

2. General use of school-related electronic communications (applies in and out of school)

- School e-mail accounts and the school web page should not be used for anything other than school communications and activities.
- Staff must not visit websites contain obscene, hateful, illegal, inappropriate or other objectionable materials
- Staff must not make or post indecent remarks on the internet, or send or receive material that is obscene, hateful, illegal or inappropriate or which is intended to annoy, harass or intimidate another person
- Staff must not represent personal opinions as the views of the school.
- Staff must not use digital communications to communicate with pupils or parents in an inappropriate manner (for instance, using email accounts, personal mobile phones, or communication via social networking sites)
- Staff must not take part in any activity which discusses school matters or is likely to adversely impact on the reputation of the school or undermine confidence in any person's professional abilities.
- Staff must report any concerns about misuse of ICT in line with the "Response to Incidents of Concern" sheet (displayed in the staff room).
- Staff must use their school e-mail account (office365) containing a disclaimer message for all school-related communications. E-mails should be written with the same standards and conventions as printed letters.
- Staff must only use the school's technologies for professional purposes relating to their role in school or for legal private purposes deemed 'reasonable' by the Head or Governing Body.
- Staff should not use the internet or other ICT for personal reasons during teaching hours.
- Staff must promote and model positive use of current and new technologies and e-safety. Members of staff can access information about e-safety from the North Yorkshire Primary ICT room and within the North Yorkshire Learning Platform and from the Learning Network; also from CEOPs and ThinkuKnow. The E-safety coordinator can also provide information, resources and guidance.

- Staff must not make inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons, including use of personal devices during teaching time or when supervising children.
- Staff must not share files which are not legitimately obtained e.g. music files from a file sharing site
- Staff must not use school or personal equipment (including phones) to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute
- Staff must not attempt to circumvent school filtering, monitoring or other security systems
- Staff must not circulate commercial, advertising or 'chain' emails or messages
- Staff must not reveal the personal information (including digital images, videos, audio and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- Staff must not use materials in a way which infringes copyright or which fails to acknowledge ownership (including plagiarising of online content)
- Staff must not transfer sensitive data (including photographs) insecurely or infringe the conditions of the Data protection Act, revised 1988**. An encrypted memory stick may be used to transfer sensitive material; this must be deleted from the stick as soon as possible.**
- Staff must not use personal devices to take photos or make video or sound recordings of school activities.

The following activities would normally be unacceptable; however in some circumstances they may be allowed e.g. as part of planned curriculum activity or as system administrator to problem solve

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone during lesson time
- accessing non-educational websites (e.g. shopping websites) during lesson time
- sharing a username and password with others or allowing another persona to log in using your account
- accessing school ICT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

3. General use of ICT

Staff:

- Must not eat or drink near computers
- Must not attempt to fix hardware problems.
- Must not install software on school computers which is not licensed to the school.
- May use hardware that belongs to them, which does not require installation of unlicensed software on the school computers (note that some hardware will automatically install "driver" software when connected to the computer – this is acceptable).
- Have a duty to protect their passwords and personal network and Learning Platform logins, and should log off the network when leaving a workstation unattended.
- Must encrypt any personal pupil data that is sent via e-mail or held on a memory stick.

- Must respect and comply with copyright and intellectual property rights.
  Have a responsibility to report any misuses of technology, including the unacceptable conduct of others, to the e-safety coordinator or Headteacher by following the Incident Response procedure outlined in the E-Safety Policy.

- Must send confidential information to the password-protected printer.

- Must make careful decisions about printing to prevent waste of resources.

- Must work with due consideration for their own and the children's health & safety when using computers.

- Must be careful to keep confidential on-screen information away from the view of children or unauthorised staff. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

- Must not intentionally interfere with the running of the school network.

I understand that the school may monitor or check my use of ICT equipment and electronic communications, and that school and/or personal devices may be confiscated if a breach of a school policy is suspected.

I agree to follow this user agreement, and understand that failure to do so may result in disciplinary proceedings in the line with the School's Disciplinary Procedure.

Signature ..... Date .....

Full Name (Printed) ..... Job Title .....