Acceptable Use of Computing at Tillingbourne Junior School:

Staff Agreement

Tillingbourne JUNIOR SCHOOL	**Review Date**	September 2025
	Date of next Review	September 2026
	Who reviewed this AUP?	Ben Stevenson

Aims & Background

At Tillingbourne safeguarding is our highest priority. This acceptable use agreement covers the use of all digital technologies while in school: ie email, internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, apps and other relevant digital systems provided by the school, Trust or Local Authority, or other information or systems processors.
This ICT user agreement also covers school issued equipment when used outside of school, use of online systems provided by the school such as VPN or webmail, or other systems providers when accessed from outside school.

This ICT user agreement also covers posts made on any non-school official social media platform or app, made from outside the school premises or school hours which reference the school or which might bring staff members or governors professional status into disrepute.
The school regularly reviews and updates all user agreement documents to ensure that they are consistent with current National guidance.

User Requirements

School employees, governors, and third party staff using school systems must comply with the requirements below. Failure to do so could possibly mean disciplinary procedures. Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may be subject to monitoring.

a. I will only use the school's ICT resources and systems for professional purposes or for uses deemed 'reasonable' by the Head, Trust and Governing Body in the line of my employment.
b. I will set strong passwords, following advice provided by the school. I will change it frequently.
c. I will ensure that my passwords are protected and safe.
e I will not allow unauthorised individuals to access email / internet / network / social networks / mobile apps / or any other system I have access to via the school or other authority or processing system.
f. I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
g. I will not engage in any online activity that may compromise my professional responsibilities.
h. I will only use the schools approved email system(s) for any school business.
i. I will only use the approved method/s of communicating with pupils or parents and will only communicate with them in a professional manner and on appropriate school business.
J. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
K. I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Head.
L. I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed. I will seek advice from the IT Manager
M. I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

N. I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.

O. I will ensure that my personal mobile phone is stored away during contact time with pupils and only used in the areas specified in the code of conduct and staff handbook.

P. I will only use school approved equipment for any storage, editing or transfer of digital images/videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.

q. I will only take or publish images of staff and students with their permission and in accordance the school's consent guidelines. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.

r. I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role, and will create a distinction between the two.

s. I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.

t. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the relevant Senior Member of Staff / Designated Safeguarding Lead.

Data Protection

a. I will only access school resources remotely (such as from home) using the school approved system and follow e-security protocols to interact with them.

b. I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

c. I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

d. I am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected.