WESTFIELD PRIMARY SCHOOL

ICT Acceptable Use Policy

This Policy was reviewed by K Beattie

July 2023

Review July 2024

Safeguarding and Child Protection Lead:	Julia Findlay (DSL)
Online Safety Lead:	Kate Beattie

Westfield Primary School

Staff ICT Acceptable Use Policy

At Westfield Primary School, we are developing our learning environment to provide a range of ICT opportunities and tools. This will empower our children to make relevant and safe choices and be flexible as they learn, in line with our school's vision.

Overview

The use of ICT has become an embedded part of outstanding and creative teaching and learning. The internet provides a wealth of teaching resources that can motivate and enthuse children and support teacher knowledge.

This policy has been formulated to cover appropriate use of ICT resources and equipment used by staff both at school, and when using school equipment off site.
The aim of this policy is:

- To ensure staff and students benefit from internet access, with clear guidance on safe and acceptable use.

- To ensure that staff benefit from all opportunities offered by the internet to provide resources that will develop pupils' learning.

- Provide guidance to staff about the acceptable use of mobile technologies, both the school's and personal items that are brought into school.

Protection of School
ICT facilities must not be used that bring Westfield Primary School into disrepute or ways that a reasonable person may consider offensive. Specific examples of inappropriate use are emails containing aggressive, abusive or libellous messages (for example, on social networking sites), or internet browsing of sexually explicit material. Accidental access to inappropriate material should be reported to Safeguarding and child protection Lead (Julia Findlay) immediately.

Software applications or updates must not be installed unless the necessary licences are held and the application/update has been approved for use on the school's network by an authorised member of the school.

Protection of Staff
The person logged on to a computer will be considered the person using it. For this reason, you should always log out or lock your computer when you are not using it. This behaviour should be similarly modelled towards the children.

Staff should ensure that any online activity, both in school and outside school, will not bring his/ her professional role into disrepute including social networking sites (for

further clarification see Social Media Policy). Security settings should be set at the highest possible level. For support with how this can be achieved, please see Computing Lead (Kate Beattie).

No comments relating to any aspect of school should be made, discussed or "liked". If this protocol is not followed, you may be leaving yourself liable to disciplinary action.

Personal Computer Security Policy.
It is the responsibility of each PC user to take all responsible precautions to safeguard the security of personal computers and the information pertaining to the school on it. This includes protecting it from hazards, including spilling liquids, not allowing unauthorised users access to the machine and only using approved software. Where information is derived from a source outside the school on an external media, it should be subjected to a virus scan before opening the document. All passwords are confidential and should not be shared with anyone other than Computing Lead or SLT.

Portables
Special consideration should be given to the protection of portables such as laptops, Chromebooks, webcams, digital cameras and camcorders, as these are more open to theft and physical damage. Laptops & Chromebooks are covered under the school insurance scheme at home and whilst in transit. However, if they are left in an unattended vehicle for any length of time, they are not covered. If they are stolen from the classroom, they will not be covered as "walk in theft" is not covered, there must be evidence of a break in.

Laptops & Chromebooks are the property of school and should contain school related information/ planning only and therefore the school reserves the right to access all information files. Laptops & Chromebooks taken home should only be used by the member of staff, not partners or other family members.

Virus Protection
Westfield Primary School uses virus protection software on all networked computers. The software is configured to intercept viruses in email attachments and files downloaded from the Internet. The software is regularly updated to ensure that the most recent detection profiles are available. Anti-virus software is also on the laptops & Chromebooks to cover them when used away from the school network.

Wherever possible, staff must use the remote server to complete work at home. USB sticks must be an encrypted USB stick provided by school, but these should only be used in extenuating circumstances discussed with Kate Beattie or a member of the senior leadership team.

Although software provides assurances, the software should not be a substitute for extra vigilance when using email and internet systems. The school reserves the right to delete suspect e-mail; e-mails containing inappropriate material or references, or containing attachments, which are inappropriate or containing viruses.

Taking and Storing Photographs of Pupils
Staff are to use the available school digital cameras when taking photographs of pupils. Personal devices should never be used to take photographs of pupils, including digital

cameras and mobile phones. All staff must completely adhere to photo permissions documents sought for each child.

School E-mail

Every member of staff has an email account. This should be used for any work-related emails. Each class is also assigned a school email address, all of which have the same password. Utmost professional conduct must be shown when communicating with parents.

Social Media

For the academic year 2022-23, the school are starting to use a twitter account. This will be moderated by Kate Beattie. This account must be used only for school matters and never used to interact with any other profiles. Any messages received to the account must be discussed with Kate Beattie or a member of the senior leadership team before any responses are made.

Sanctions

Any member of staff alleged to be accessing inappropriate material or have this stored on his/her laptop/Chromebook/class computer may face suspension/ disciplinary action as part of an investigation. The Lead DSL and Personnel will be informed and Surrey County Council guidance adhered to. The Head teacher & Lead DSL must consider the allegation and determine the appropriate way forward. (see Allegations of Abuse Against Staff Policy)

Westfield Primary School ICT Acceptable Use Policy
I have read this policy and agree to these safety restrictions.

Signed_____

Print_____

Date _____