Binfield CE Primary School (VA)

Acceptable Use Policy for Staff

(Definitive)

Date Created: October 2013

Date Last Reviewed: April 2026
Date Last Updated: April 2026

Status:

Next Review Date: March 2027

Acceptable Use Policy for Staff

This covers use of digital technologies in Binfield CE Primary School (VA): i.e. e-mail, internet, intranet and network resources, learning platforms, software, mobile technologies, equipment and systems. Any questions you may have regarding e-safety or the acceptable use of the ICT facilities in school should be directed to the Head Teacher in the first instance.

Using the ICT Facilities in school

Staff must only use the Schools digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Headteacher, or (Computing Subject Leader.)

Staff should ensure that their login details (including passwords) are **not shared with anyone outside of school staff.**

Staff must not allow pupils to use a laptop that has been assigned to them. Staff should not loan their School laptop to anyone else, including family members.

Staff must have their laptop at work each day it is required. For class teachers this will most likely be daily.

Staff must not allow unauthorised individuals to access e-mail/internet/intranet/networks or systems. Visitors to the school who require access to the internet can only do so with the permission of the headteacher.

Staff must not connect a computer, laptop or other device to the network/internet that has not been approved by the School and meets its minimum security specification.

Staff must not use personal digital cameras or the camera facility on a mobile phone for taking or transferring images of children and young people or staff. Staff should use school designated equipment only for this purpose unless for a specific purpose whereby written permission has been obtained in advance by the Headteacher.

Using the Internet

Staff must not use the ICT facilities in school for personal reasons at any time when they are not on a timetabled break, including during directed time after school.

Staff must only use the school e-mail system for any school business. Staff must not use a personal web mail service such as Hotmail, Yahoo or Gmail to contact professionals, partners or parents/carers regarding school matters.

Staff must not browse, download or send material that could be considered offensive to colleagues or to any other individuals.

Staff must report any accidental access, receipt of inappropriate materials or filtering breaches to the Computing Subject leader/TSI. Depending on the material accessed, they may pass that information to the Headteacher.

Staff must not download any software or resources from the internet that can compromise the network or are not adequately licensed. If software is required for a legitimate purpose, staff will contact the subject leader who will advise on how to proceed.

Staff must not engage in any online activity that may compromise their professional responsibilities.

Staff must be aware that all internet and network usage can be logged and this information could be made available the school.

Social networking sites

Staff must not allow parents or children to add them as a friend to their social networking site nor should they add them as friends to their social networking site. Any staff who are also parents, must take individual advice from Head Teacher; however, the School would advise against this activity as it almost impossible to delineate the two roles clearly.

At home, staff must ensure that any private social networking sites/blogs etc. that they create or actively contribute to are not confused with their professional role. Staff must not use these forums to make any comments in relation to the school, colleagues or students or to post any information including photographs. The School's advice is to act with extreme caution if staff choose to use such sites, and; it may be more prudent to avoid them altogether.

Staff must not access personal social networking sites e.g. Facebook, Instagram etc whilst using the ICT facilities in school.

Internet Forums

Staff must not share information about the school in internet forums as it is unacceptable and can bring the school and / or the local authority into disrepute and put children at risk. If staff see or become aware of inappropriate information about staff or children through communications with colleagues, parents or partners, they must alert the DSL. Staff must keep this information confidential in line with the Data Protection act and within the school's Safeguarding Policy. However there may be times when they are required to disclose information to an appropriate authority such as the Police or Children's Social Care. In such cases, staff can seek advice from the school's Safeguarding officer or Local Authority HR.

Generative AI

Generative AI is fairly recent tool available to staff. As this current time, our advice is to act with extreme caution when using this as part of their professional role. Staff should ask themselves: is it safe? Ethical? And accurate/reliable? Staff should only use Co-Pilot and should not upload pupil's work for assessment purposes or anything else. Staff should also ensure they adhereto GDPR & confidentiality guidance and never insert personal details into AI. As we learn more, a detailed policy will be developed.

Staff must ensure that they are aware of digital safeguarding issues so that they are appropriately embedded in their practice. If they are unsure of digital safeguarding issues, they should contact the school's Safeguarding officer or one of the computing lead for more information.

Staff should be aware that failure to comply with the Acceptable Use Policy (AUP) could lead to disciplinary action.

Staff must take responsibility to ensure that they remain up-to-date and read and understand the School's most recent Acceptable Use Policy (AUP).