Staff Use of ICT
Acceptable Use Policy

Copnor Primary School Breakfast/After-School Clubs seek to embrace the use of ICT to enhance teaching and learning in the school. This guidance on appropriate use of ICT has been put together to fulfil government requirements. All staff with access to the ICT network are required to read and sign it.

Use of the Internet

- All use of the internet at school should be primarily to enhance teaching and learning or for administrative use.
- It is understood however that staff may occasionally need to use the internet for personal reasons. Such use should be limited to outside of lesson time for teaching staff and during breaks/lunchtimes for support staff.
- Internet access in school can be monitored. Appropriate County filtering systems are in operation for both staff and pupils.
- The accessing of inappropriate and indecent materials from the internet or via e-mail will result in disciplinary action being taken.
- Staff must use caution when posting information online including on social networking sites and blogs.
- Staff must not post material damaging the reputation of the school or which could cause concern about their suitability to work with students. Staff posting material which could be considered inappropriate could render themselves vulnerable to criticism or allegations of misconduct and if it brings the school into disrepute they will face disciplinary proceedings. *Staff must not be 'friends' to, or communicate with, current students on 'Facebook', 'Instagram', 'Twitter' and other social network or similar websites.*

Use of E-mail

- Use of school e-mail addresses is encouraged for correspondence with the school and externally as required. Staff will not communicate with students via email.
- Email should be treated as inherently insecure. You need to be careful of the language you use in all correspondence. Please be considerate with numbers of emails sent, ensuring that all methods of online communication (e.g. online noticeboard) are used appropriately.

Use of the ICT network (including tablets and Tapestry in EYFS)

- Each member of staff has a unique login for the network. It is recommended that you change your password for network access regularly (at least once a term). Passwords should not be obvious, and ideally include alpha and numeric characters and a mix of upper and lower case. Passwords should never be divulged to other staff and especially pupils. Accounts will lockout after five incorrect password attempts.
- When using the ICT suite with pupils, staff are expected to be in the room at all times and are responsible for ensuring that use of the facilities by pupils is appropriate. Staff may be held responsible for any damage that occurs whilst your class is in the ICT suite.
- It is the responsibility of all staff to ensure that pupils do not have access to confidential data, SIMS and must therefore be vigilant in their security measures e.g. locking out the computer when leaving the room for a short period of time.
- Data stored on the network is backed up regularly; staff should however ensure that data on removable media and laptops is also backed up.
- Please note that your network activity (including home area) can be monitored.
- It is vital that network security is not compromised. Removable media can be brought into school, however these should be used with caution as they may include viruses or other malicious software. The ICT Technical Team has the right to confiscate any such media if they believe that network security may be compromised.
- ICT devices not purchased by the school should not be connected to the school's ICT network, except with prior approval in exceptional circumstances. Purchases of new ICT hardware should be approved by the ICT Manager.
- Software loaded on school owned ICT devices must be appropriately licensed. Budget holders have a responsibility to ensure that software purchased is licensed appropriately. Software installations on networked PCs should be approved by the ICT Manager.

- A separate agreement is in place for staff that have been designated a school laptop. Other equipment may be taken home at the discretion of the line manager/Head of Department.

E-safety

- Whilst access to unsuitable internet content is minimized by filtering software, this can never be completely eliminated. It is therefore important that staff recognize their duty of care to ensure that pupils do not access or search for inappropriate website content. In addition pupils should not give out personal information online (including through e-mail).
- For reasons of child protection, pupil data and photographs should not be stored online unless in a secure area.
- Use of Tapestry in EYFS is approved but the tablets assigned for that should only go home with the prior consent of the EYFS manager, and under no circumstances should any information or images from the Tapestry tablets be downloaded to personal computers/smart devices.
- As soon as photos from the Tapestry tablets have been uploaded to the online learning journeys they should be deleted from the tablets.
- Staff accessing inappropriate material or using ICT facilities irresponsibly will be subject to disciplinary proceedings and police involvement may result.
- If you suspect that illegal content has been accessed on a computer, the workstation should be immediately powered down and secured. Do not attempt to check whether content is illegal by accessing it and contact a member of Senior Management immediately.
- If a staff member has any reason to suspect suspicious activity they must report this to a member of senior management immediately, even if they have no proof.

I have read through the "Acceptable Use Policy" regarding staff use of ICT and agree to the above expectations.

Print name: _____

Signature: _____ Date: _____