

YORKMEAD JUNIOR AND INFANT SCHOOL (NC)
COMPUTER, INTERNET AND E-MAIL ACCEPTABLE USE POLICY
(ADULTS)

Yorkmead school is committed to safeguarding and promoting the wellbeing of all children, and expects our staff and volunteers to share this commitment'.

The School's computer system is well established and plays an integral part in the education of pupils and others at Yorkmead. Access to the Internet is provided for purposes of educational research and learning. The following policies for staff provide rules and safeguards to ensure appropriate use of the Internet, both on and off site whilst using school equipment.

Before accessing the Internet staff, pupils and other users should be made aware of these policies.

By accessing the school network and the Internet, users agree to the school's terms and conditions:

- To refrain from accessing any links, Web pages or other areas of the Internet that would be considered offensive because of pornographic, racist, violent, illegal, illicit or other content.
- To monitor and appropriately reject inappropriate materials, links, dialogues and information accessed/received by the users.
- Courteous and appropriate language should be used at all times. Obscene, harassing and abusive language is not permitted. If any such language is received it should be reported immediately to a member of the senior leadership team.
- Users should avoid downloading materials where the copyright forbids use in schools. This includes games, music, graphics, videos or text materials. Such copyright materials should not be posted or distributed by users.
- Users are not allowed to copy copyrighted media onto the school network.
- Personal information, including names addresses and telephone numbers of users or others should be kept confidential, in a locked unit and on the SIMS.NET.

- Users wishing to install software must have the permission of the Head Teacher. The software must be installed by the Network Manager and not the individual user.
- The discovery of any viruses or other potentially damaging software must be reported to the Network Manager immediately and the computer not used until remedial action has been taken.
- Computer, monitor and software settings on any school computers may not be changed without permission.
- Users must only log-in using their own username and password which is to be kept confidential. Users should respect others work and not attempt to access other people's work on the network by using either aliases or passwords that are not assigned to the user.
- The entire network is protected by anti-virus software. Staff are advised to use anti-virus software on home computers and laptops. If a virus is reported on screen the Network Manager should be informed immediately.
- The Network Manager carries out daily network backups. However, users should save their own work and use appropriate file management techniques at all times. Staff data should always be saved to their network homedrive/ staffcommonarea or common network areas. USB pen drives should be backed up by the individual to the appropriate network area/s as outlined above
- School laptops are issued to staff for use by employee's of Yorkmead School **ONLY**. This laptop is for the assigned staff member only and shouldn't be used by any other person whilst offsite.
- Staff must not accept pupils as contacts/friends on any social networking sites.
- All violations which are received off the school premises and alerts the network Manager and SLT if any violation has occurred.
- All information that is taken off site or produced off site for school use must be encrypted. Teaching staff are issued with an encrypted memory stick and all data needed out of school should only be stored on this memory stick. Use of your own memory stick is not permitted to store sensitive data which could contain staff/pupil information whether written or photographed.

- Violation of any of the terms of this agreement could lead to a verbal or written warning and/or further action being taken.
- Impero remote monitoring software is installed on all school computer devices and used to monitor the internal and external usage of all school owned equipment. Inappropriate use of any school device will be reported to the SLT with the possibility of disciplinary action being taken, should this be necessary.
- By signing this document you are accepting that you understand that the Network manager and SLT can access your computer remotely at any time should they feel it necessary to do so.
- This document is subject to change at any given time. Staff will be informed should changes need to be made.
- Failure to sign this document will result in forfeiting your laptop back to the school .This also means all external access to information from the school network will no longer be allowed. This includes the use of pen drives and all other forms of media/cloud storage or remote access which could be used to store or retrieve school data.
- Access to the school network using VPN/Home Access plus must be used in a confidential manor and not left unattended when not in use. Sensitive information should also not be opened in the view of any other person not authorised to access.

This is to comply with the Data Protection Act .

This policy will be reviewed in July 2018.

Signed: _____ Chair of Governors

Dated: _____