IT Usage Policy

Rudyard Kipling Primary School

May 2018

Introduction

ICT and the Internet open up a vast source of information and learning opportunities previously unavailable to children and staff.

At Rudyard Kipling we encourage children to make the best possible use of all ICT resources, including enabling them to further their own learning using the Internet.

We believe that ICT skills are a major factor in enabling children to be confident, creative and independent learners. We focus on developing the skills necessary for children to be able to use information in a discriminating and effective way.

General Statement

Enquiries

Information about the school's IT Usage Policy is available from the School Office and the school website. Information about the General Data Protection Regulations (GDPR) can be obtained from the Information Commissioner's Office (Helpline **0303 123 1113** or **01625 545745**, website http://www.ico.gov.uk). Our Data Protection Policy details how we comply with the GDPR.

Purpose of this Policy

To establish rules and guidelines for staff, pupils and parents on the safe use of ICT in the school and to explain and demonstrate the systems in place for the management of access to the Internet.

Staff responsibilities

Every member of staff is given a set of user names and password to log-in to the various parts of the school system. These details should never be shared.
Staff members are provided with logins for the following systems where required to perform their job functions:

- School Network
- SIMS System (School Information Management)
- Email/Office 365/OneDrive
- CPOMS (system for monitoring child Protection, safeguarding, SEND, attendance, behaviour etc).
- Prowise Presenter (class presentation software)
- Class Dojo (online behaviour reward system)
- Google Classrooms (to create documents, activities and discussions for use in Computing lessons)

Guest log-in details are available at the school office for supply staff as part of a 'Supply Pack'.

Our classroom computers run the Windows 10 operating system and are updated regularly to ensure they have the latest security patches. We use Sophos antivirus software to scan files and manage external drives/cameras and Internet access is filtered using the 'Smoothwall' proxy server system.

Rudyard Kipling Primary School and Nursery
IT Usage Policy

'Together we will help each other to achieve our best'

It is all staff members responsibility to ensure that the data on our systems remains secure. Passwords should never be shared.

All computers should be locked when they are left unattended. This can be done by pressing the 'Windows' key and the 'L' key simultaneously. As a backup, all computers will automatically lock after ten minutes.

Memory Sticks/OneDrive

All are set up with a 'OneDrive' account. This can be used to store and transport files and resources from computer to computer. It also allows for Microsoft Office to be created/edited/shared online. The account is password protected and can be accessed on a wide variety of electronic devices. Staff may use a school-supplied encrypted memory stick/USB drive which must be access authorised by IT support for each machine on which it will be used. We encourage staff to use OneDrive instead of this method. Visitors to our school who bring resources on memory sticks (for example a visiting speaker for assembly) will be able to access the resources on their USB drives by presenting them to the school's IT assistant who will access the files using the one machine in the school which allows for general USB device access.

Laptops.

A few staff may need to use school laptops at home. These machines will be set up with password protected VPN software which will allow them to access their school resources at home. No documents should be saved on the laptop itself.

Home computers.

Staff's own home computers may be used to work at home but should not be used for the storage of any personal data regarding pupils or staff of the school. Any references to pupils on lesson plans etc. should include no more than the pupil's initials. Documents which include personal data or sensitive personal data should be created and edited within the OneDrive system and should not be downloaded to home computers.

Cameras

Each class is provided with a digital camera. There are also 4 mini video cameras which can be booked out for use by staff. In addition to this, our 50 Nexus Tablets are equipped with front facing cameras which can take still images or video footage. Staff may take photographs of children and their work to keep as evidence of learning and for displays in the school. Photos of children for inclusion on the school website, reception display screen, prospectus or in local newspapers can only be used if their parents have given explicit written consent or this has been gathered using a secure electronic means (such as a Parentmail form). See the Use of Images policy for further information.

Email

All staff are provided with a Microsoft Office 365 Email account. This should be used for all school business. The email system can be accessed from any internet-enabled computer including most mobile devices. In most cases the Email system will be accessed through an Internet browser. On mobile devices it can also be accessed using an App. In these cases an extra level of setting up will be required to ensure the device is encrypted and sufficiently secure. This can be arranged by contacting B&H ICT support via the school business manager. All personal and sensitive information should be encrypted whenever it is sent to anyone outside the school 365 email environment **N.B. ONLY B&HCC Primary Schools use the 365 email environment.**

Rudyard Kipling Primary School and Nursery
IT Usage Policy

'Together we will help each other to achieve our best'

Red and Amber data should only be sent by email if it is encrypted by typing [encrypt] in the subject title or body of text

Red data (those that contain very personal details)
- EHCPs
- Education Psychologist reports
- Education Welfare Officer reports
- Medical records
- Personnel records
- SEN registers

Amber data (data that contains personal data that if lost could identify individuals)
- Names and Addresses
- Parental contacts
- Pupil reports
  Exam results

Green data can be sent by email (data that does not identify individuals)
- Lesson plans
- Class lists (only showing initials and forenames)
- Curriculum plans
- General marking

Pupil Access

Children are able to access locally installed applications, World Wide Web pages and other approved Internet resources using the computers in our Computing Suite (running on the Windows 10 operating system) or Nexus 7 tablet computers (running on Android 4 operating system). Children's access to online resources is limited and made safe through use of 'Smoothwall' managed firewall software. Children are given Google Logins for use with Google Classrooms. Using these logins children are taught to use Email and other online resources responsibly. Children's use of Email is limited to communicating with other children within their yeargroup. Children cannot send or receive emails to or from individuals from outside of the school's domain. The Use of Google Classrooms also allows children to create and collaborate on word processor documents, spreadsheets, presentations and artwork online. Children are also given logins for 'Sumdog' an online mathematics programme which allows children to play games which include maths questions tailored to their ability level.

Staff are responsible for explaining the risks carried by inappropriate use of the Internet and the expectations of children when using the Internet in school, as well as highlighting safety precautions for Internet use outside of school.

E-safety advice and information is taught to all year groups throughout the year and is built in to our Computing and PSHE curricula.

Teachers will have access to pupils' Google Classroom pages and communication. Any inappropriate or bullying behaviour will be reported to senior management.

Teachers are also expected to be aware which children are not permitted to have their images published on the website or elsewhere. A list of these children is kept in the school office.