Sutton in Craven Community Primary School

Acceptable Use Policy

ICT & Technology

Our school is a place ‘where learners grow.’

A kind community where the worth of everyone is nurtured and celebrated.

We are rooted in a love of learning and building the confidence and courage to be ourselves.

Together we flourish to be the best we that we can be.

Approved by:	Business Group	**Date:**	
Last reviewed on:	Summer 2022		
Next review due by:	Summer 2025		

This agreement is designed to ensure that all members of staff are aware of their professional responsibilities when using any form of technology. Technology relates to ICT systems, hardware, software, internet, email, cloud based learning platforms, mobile devices, cameras, laptops and memory devices.

Members of staff:

- Must only use the school's technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body. It is a criminal offence to use an ICT system for uses other than those permitted by its owner. Staff should be aware that their use of the school digital technology and communications systems may be monitored.
- Must only use approved, secure school systems for any school business. Staff may use their personal equipment to access cloud based data and use this system to avoid school data being stored directly on personal devices. If given exceptional permission to store any data, they undertake to delete all school information once they have finished doing a task. All student data must be kept within our Google domain and must not be stored locally on phone, tablet or laptop. Worksheets, presentations etc may be stored anywhere provided they do not contain student's personal information. Photographs must be moved to Google Drive as soon as possible and any local copies deleted. All devices set up to access our Google domain must be password protected.
- Staff only use school subscriptions (like tapestry) over a secure connection (https) e.g. a private network at home rather than an open public network.
- Must not browse, download or send material that could be considered offensive, and should report any accidental access of inappropriate materials to their line manager. This includes material that is linked to radicalisation and extremism, racial discrimination, is sexually inappropriate, promotes violence, grooming, or any other actions which bring the school into disrepute.
- Have a duty to protect their passwords and personal network and learning platform logins, and should log off the network and learning platform when leaving a workstation unattended. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- Must not install any software or hardware without permission from a technician or the ICT leader. Staff must be vigilant not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if they have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- Are not permitted to use personal portable media for storage of school related data/images (e.g.USB stick) without the express permission of the Headteacher. If USB sticks must be used, the user should ensure it is scanned for viruses.
- Should ensure that personal data (such as data held on SIMS) is kept secure under password protection and is used appropriately, whether in school, taken off school premises, or accessed remotely. Personal data can only be taken out of school when authorised by the Headteacher or Governing Body.
- Are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, including when on external trips/visits. With the written consent of parents(on behalf of parents) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. Digital images are easy to capture, reproduce and publish and, therefore, misused.
- Should ensure that their use of social networking sites, such as Facebook and Twitter, does not question or bring their professional role into disrepute.
- Are advised to consider, and set appropriately, their privacy settings on such sites.
- Should consider the appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
- Should not communicate with individual pupils, in relation to either school or non school business, via social media. Members of staff should only communicate with pupils using the appropriate LA/school learning platforms or other systems approved by the Headteacher e.g. google app for education.
- Are not permitted to contact or communicate with pupils, parents or conduct school business using personal email addresses or telephones, without specific permission from the Headteacher.
- Should not give out their own personal details, such as telephone/mobile number or email address, to pupils. School email addresses should only be used.
- Must ensure that all electronic communication with pupils and staff is compatible with their professional role.
- Must promote and model positive use of current and new technologies and e-safety.
- Must respect and comply with copyright and intellectual property rights.
- Have a responsibility to report any misuses of technology, including the unacceptable conduct of others, to the e-safety coordinator or Headteacher.

I understand that I am responsible for my actions in and out of Sutton CP School:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.
- I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:
Signed:
Date:22/03/17 ____________

Appendix

Internet Safety Awareness for parents

Parents are advised on the latest developments to ensure that they are aware of how to keep their children safe on the internet at home. Guidance on the responsible use of Facebook and other social networks by parents in connection to school will be provided.

Digital and Video Images of Pupils

Parental permission is sought when children start school regarding the use of photographs of pupils on the school website and in the local press. These details are available on the school
system. It is the Class Teachers responsibility to be aware of which children's photos can't be used. When on school trips the group leader must make clear to helpers that they are only permitted to take photographs of their own child.

School Website

Our school website promotes and provides up to date information about the school, In order to minimise risks of any images of pupils on the school website being used inappropriately the following steps are taken:

- Group photos are used where possible, with general labels/captions;
- Names and images are kept separate – if a pupil is named their photograph is not used and vice-versa; Only first names of children will be used.
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.

Storage of images

Digital and video images of pupils are taken with school equipment only. Images are stored on a centralised area on the school network, accessible only to teaching staff. Photographs of pupils are removed when they leave the school.

Social Software

Chatrooms, blogs and other social networking sites are blocked by the ISP – EXA networks - so pupils do not have access to them in the school environment. Children have controlled access to in-school chatrooms through our secure web services.

Sanctions

We regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Internet Safety Education for pupils. Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school's discipline policy and child protection procedures. Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

(This policy has been drawn up by the staff of the school under the leadership of the ICT Co-ordinator in line with North Yorkshire Acceptable Use Agreement.)