Willingdon
COMMUNITY SCHOOL

Acceptable Use of ICT for Staff, Approved Guests & Volunteers Policy

Date adopted by the Governing Body: 7th February 2019

To be reviewed: February 2019

Staff Responsible: Headteacher / DSL

Link Governor: Safeguarding Governor

Willingdon Community School Staff ICT Acceptable Use Policy

This Acceptable Use Policy is intended to ensure:

- ***that staff, volunteers and approved guests, such as ITT, will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.***
- ***that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.***
- ***that staff are protected from potential risk in their use of ICT in their everyday work***

Willingdon Community School provides a range of ICT resources which are available to all staff. In order to ensure the safety of both staff and students, it is important that all staff follow the guidelines detailed below.

Terms of Acceptable Use:

Application of policy: This policy applies to all staff of the school and volunteers, including approved guests regardless of their use of ICT systems

School Email

Every member of staff is provided with a school email address. The email system can be accessed from both the school computers, and via the internet from any pc.

The sending of emails is subject to the following rules:

- **I will always communicate in a professional manner.**
- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature, terrorist and extremist material are not permitted.
- Sending of attachments which contain copyright material to which the school does not have distribution rights is not permitted.

Limited personal use of the email system is permitted, provided that it complies with the guidelines set out in section 4 of this policy, and that any content complies with the rules above. Staff should keep levels of personal email to a minimum.

All email within the school is monitored, and email accounts can be checked in order to ensure compliance with the above rules.

All staff should be aware that email is not a secure communications medium, and therefore careful consideration should be given before the transmission of confidential files or staff / student data.

Staff volunteers and approved guests are not permitted to send via email any information which is covered by the Data Protection Act, without prior written authorisation from the schools data protection officer.

Other than the examples listed above, use of email should comply with the ESCC E-mail use policy.

Internet Access

The school provides internet access for all staff and students in order to allow access to the wide range of content available.

The schools' internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasion it may be possible to view a website which is inappropriate for use in a school. In which case the website must be reported in writing (e-mail) to the ICT helpdesk.

It is not permitted to attempt to access, on any device, pornographic, illegal, sexist, violent, racist, extreme, terrorist or other inappropriate material in school.

Members of the ICT Support Team have access to an unfiltered internet connection. Access is still only permitted to appropriate websites, unless directly instructed by the Headteacher.

The use of online real-time chat rooms is banned, unless specific permission is sought from the Head Teacher.

No member of staff may download any software from the internet for installation onto a school computer system without prior written authorisation from the Headteacher.

In addition to the examples listed above, use of the internet should comply with the ESCC Internet access and use policy.

Personal use of Equipment

The ICT provisions provided by the school are for work relating to the School. However, the school acknowledges that, on occasion it may be necessary to use the ICT equipment for personal use. This is permitted provided that:

- Any activities carried out on them complies with the other terms of this policy.
- No personal applications are loaded onto any computers.
- Any activity completed on school equipment does not result in personal gain for the member of staff involved.
- The removal of ICT equipment from the school site for personal use is only permitted with the consent of the Head teacher or Business Manager. The exception to this is any equipment assigned to, and signed for by individual members of staff.

Individuals are responsible for the cost of any personal phone calls. All calls are logged and may be recorded.

All staff members are responsible for reporting their own personal use of a school computer, and any associated tax costs this has.

No technical support is provided by the school for problems arising as a result of personal work on the equipment.

Digital Photography

The school encourages the use of digital cameras and video equipment; however, staff should be aware of the following guidelines:

Photos should only be named with the students' name if permission has been sought from the parents via the image permission form. The updated list is under photo permissions on Assessment Manager.

The use of **digital photography** in school is permitted. However, images of students must be downloaded to the school network and removed from the camera before it leaves the school site.
All photos should be downloaded to the school network

Security

Each member of staff is allocated a username and password. Staff are responsible for ensuring their password remains a secret and their account is secure. Staff are not permitted to write their password down.

Under no circumstances should a student be allowed to use a staff computer account, unless being directly supervised by the account owner for the purposes of curriculum use. When any pc is left unattended, it must either be logged off or locked. No member of staff may use a computer which is found logged on as someone else, it must be immediately logged off.

Passwords are recommended to be changed regularly. Staff will only access areas of the schools' computer systems to which they have been authorised access.

File Storage

Each member of staff has their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives. **Staff must not access, remove or otherwise alter any other user's file, without their express permission.**

All staff should be aware that all files must be stored on a network shared area in order that they will be backed up. Files lost from a USB key are not recoverable.

Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files.

Any files stored on removable media must be stored in accordance with the following:

No school data is to be stored on a home computer, or un-encrypted storage device.
No confidential, or School data which is subject to the Data Protection Act should be transferred off site using unsecured email.

Any student data will be kept private and confidential, except when it is deemed necessary by school policy or law to disclose such information to the appropriate authority.

Mobile Phones

All phone contact with parents regarding school issues will be through the schools' phones and not through personal mobiles unless in an emergency on a school outing.

Social networking

Please refer to the Schools Social Media Policy.

I can confirm that I have completely read and understood the Acceptable Use of ICT for Staff and Approved Guests and Volunteers Policy

Signed:_____

Dated:_____