Staff and Volunteer ICT Acceptable Use Policy
(including use of email, the internet and off-site use of ICT)

Adopted date:	**To be approved at next FGB on 26.03.20**
Signature of Headteacher:	
Signature of Governing body:	

This policy should be read in conjunction with the school's Safeguarding Policy and Child Protection Procedures.

West Moors Middle School is a Rights Respecting School, and this policy addresses many of the Articles of the United Nations Convention on the Rights of the Child, specifically Articles 17 and 36:

- **Access to information from mass media:** Every child has the right to reliable information from the mass media. Television, radio, newspapers and other media should provide information that children can understand. Governments must help protect children from materials that could harm them.
- **Exploitation:** Governments must protect children from all forms of exploitation that might harm them.

Throughout this policy 'staff' should be taken to mean staff and/or volunteers.

Purpose of this policy

To ensure:

- that school ICT systems are protected from accidental or deliberate misuse that could put the security of the systems and/or users at risk.
- that staff will be responsible users and stay safe while using all aspects of ICT.
- to provide guidelines and standards to ensure the secure, effective and acceptable use of ICT both in school and off-site.
- to ensure that users are aware of the legal and/or professional consequences attached to the inappropriate use of the facilities.

General Principles

- The school's ICT systems are for educational and administrative purposes. Staff are not permitted to use the school's ICT systems for personal or recreational use.

- Staff must be aware that they are responsible for the security for any data they take off-site whether on a laptop PC, hand-held device or on removable media.

- Staff are responsible for all content stored under their name on the ICT system and for any information sent from their account. This means every account, including email accounts, may only be used by the person to whom it is assigned and is not to be shared with anyone for any reason. Staff will be held responsible for any illegal activity that occurs from the use of their account. For this reason staff will not disclose their username or password to anyone else or try to use any other person's username and password.

- Staff will immediately report any illegal, inappropriate or harmful material or incident as soon as they become aware, to their line manager or in his/her absence or if relating to their line manager to their manager's manager.

- West Moors Middle School retains the right under the Regulation of Investigatory Powers Act (RIPA) Act 2000 to access all information held on its information and communications facilities, to monitor or intercept any system logs, web pages, E-mail messages, network account or any other data on any computer system owned by West Moors Middle School. This will be for the purposes of preventing, detecting or investigating crime or misuse, ascertaining compliance with regulatory standards and West Moors Middle School policies, or to secure effective system operation.

- West Moors Middle School reserves the right to disclose the contents of any email or other electronic communications to comply with or assist law enforcement officials or legal authorities. It should be noted that email messages (deleted or otherwise) may be treated as written evidence in law.

- Staff must use school ICT systems in a professional and responsible way, including ensuring that there is no risk to their safety or to the safety and security of the ICT systems and other users.

- Teaching staff (which includes TAs) will recognize the value of the use of ICT for enhancing learning and will ensure that students/pupils receive appropriate opportunities to gain from the use of ICT.

- Teaching staff will, where possible and relevant, educate the pupils in the safe use of ICT and embed e-safety in their work with young people.

Acceptable and professional use of ICT

Staff will at all times be professional in their communications and actions when using school ICT systems. This will include (but is not limited to):

Social Networking and Code of Conduct

- only using chat and social networking sites in school for educational purposes and with prior permission of the Headteacher.
- following Dorset's Social Networking policy and Code of Conduct at all times (including off-site and in their own time) which will mean that they do not take part in any on-line activity that may compromise their professional responsibilities or the reputation of the school.

Email addresses and use of email

- carrying out all school based correspondence *(including that with students/pupils/parents/ carers/colleagues)* using official school systems; this includes using a school email address in the format name@westmoorsmid.dorset.sch.uk. Any such communication will be professional in tone and manner. Email should be carefully constructed as per other types of correspondence and users of the email system are responsible for ensuring that they are acting in compliance with legal and acceptable use conditions.
- not using school email address for personal correspondence *including private internet shopping.*

Data Protection including storage of information on portable devices

- not accessing, copying, removing or otherwise altering any other user's files, without their express permission.
- any information regarding children that is held on school based property e.g. laptop will be password protected and held on the machine/device for the shortest time possible. A master copy of the data must be maintained on the school servers and updated as soon as practical whenever the data on the portable system is changed.
- laptop users assessing the risks of taking data with them to meetings or to work on at home. If they do choose to do so then particular care should be taken during transportation to prevent systems being stolen from vehicles or by leaving items unattended, even momentarily.
- users being aware that they are responsible for the security of the data they are taking away, whether on a laptop PC, hand-held device or on removable media (*e.g. USB Drive/CD/DVD*).
- at all times following the guidelines laid down by the School/LA Personal Data Policy and the Data Protection Act .

Using of equipment not owned by the school, including staff's own devices

- **not connecting personal portable devices not owned by the school, ie laptops, iPads, Smart Phones, directly or indirectly to the school network without prior knowledge and consent of the Head Teacher.**
- only using privately owned equipment for communications relating to work in the case of an emergency where there is no other viable option. *NB, this means that except in an emergency staff should not telephone parents using their own mobile phone or landline.*
- not holding any data (which includes images) regarding children on any devices not owned by the school.

Care of equipment

- not installing or attempting to install programs of any type on a machine, or store programs on a computer without the prior consent of the Headteacher/IT coordinator.
- not disabling or causing any damage to school equipment including portable devices such as laptops.
- reporting any damage or faults involving equipment or software, however this may have happened.
- ensuring that strong security measures are introduced to all portable equipment, as soon as practical after purchase, particularly if the equipment has networked access capability.

Internet security

- only by-passing the school's internet filtering system by using the RM Proxy Server system (which may be monitored) using a 'user name' and password provided by the Headteacher/IT coordinator.

Preventing the Spread of Malicious Software (Viruses)

- not opening any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs
- not transmitting any files which they know to be infected with a virus.
- ensuring that an effective anti-virus system is operating on any computer which is used to access West Moors Middle School ICT facilities.
- taking all other reasonable steps to prevent the receipt and transmission of malicious software, including ensuring that portable hard drives (*including 'memory pens'*) are only used to transfer files between computers that have an effective anti-virus system operating on them.

Downloading/uploading information

- not downloading/uploading or accessing any materials which are illegal *(including still under copyright, such as some music) ,* inappropriate for a school or which may cause harm to others.
- not, without prior permission, making large downloads or uploads that take up internet capacity and prevent other users from being able to carry out their work; *this includes downloading films/some music.*

Images

- ensuring that when/if staff take and/or publish images of others they will do so with their permission and in accordance with the school's policy on the use of digital/video images. Where these images are published it will not be possible to identify by name, or other personal information, those who are featured.

Legislation

West Moors Middle School must ensure that its ICT systems and where applicable the supporting infrastructure complies with the relevant legislation and contractual requirements. It is the responsibility of all adult users of West Moors Middle School ICT facilities to make themselves aware

of the laws that apply to such use. The following are *some* of the areas of law which could involve liability of users or West Moors Middle School.

The Data Protection Act 1998
The Human Rights Act 1998
The Computer Misuse Act 1990
The Copyright, Designs and Patents Act 1988
The Freedom of Information Act 2000
The Regulation of Investigatory Powers Act 2000

Sanctions

Staff should note that inappropriate use of ICT, including email and working off-site either using their own equipment or the school's in an unacceptable and inappropriate manner may be treated as a disciplinary offence.