Siddal Moor
Newhouse Road
Heywood
Lancashire
OL10 2NT
Tel: 01706 369436
Email: office@siddalmoor.uk
web: www.siddalmoor.uk

Acceptable Use Policy for the Siddal Moor Sports College IT Systems

Policy updated 8th March 2018

Ratified by Governors at a meeting of the Curriculum and Standards Committee on May 2nd 2018
Ratified in its present form pending review / updates in the Autumn Term to ensure compliance with GDPR

SIDDAL MOOR

Where students ***fly high*** through the expectation of ***excellence*** in ***everything*** we do

General Principles

All users of Siddal Moor ICT services are required to follow the conditions laid down in this policy. This policy applies as follows:

- to all school owned devices, whether they are located on school premises or elsewhere.
- to all devices attached to the school IT systems either on the school site or elsewhere.
- to all members of the school community, including Governors, Staff, pupils and third party contractors working on the school's behalf, regardless of the location from which they connect to the school systems or the device they use to make such a connection.

This policy is intended to be read in conjunction with the School Social Media Policy which expands upon the basic principles outlined here as they pertain to social media platforms.

All users are expected to demonstrate a responsible approach to the use of ICT resources available to them and ensure that they use technology *safely, responsibly* and *legally.*

Subject to the sections below on acceptable use, the schools equipment and the Internet may be used for any legal activity consistent with the aims, objectives and rules of the school.

All staff who wish to use ICT services provided by the school will be provided with a complete copy of this policy and will be asked to sign a declaration that they have read and understood its contents.

In the case of employees, a breach of the conditions laid down in this policy, including failure to adequately monitor the use of ICT by pupils under their direct supervision, may be considered a breach of the employee's conditions of service which could lead to disciplinary action.

The school has developed a set of guidelines for the use of IT facilities by pupils. These rules will be made available to all pupils as part of their IT lessons, before they are allowed to use facilities in school. A copy is included with this document. All members of staff who are involved in the use of IT with pupils are responsible for ensuring that pupils know these rules and if necessary explaining them and their implications to pupils.

The following job roles are referenced in this policy and these roles are currently carried out by the following staff:

IT Manager:	Mr G Beaumont
Web Manager:	Mrs C Towers
Computing HOD:	Mr A Dawson
Designated Safeguarding Lead:	Mrs T McLoughlin
SMT Member responsible for publicity:	Mr I Baird

Staying Safe

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the virtual or digital world as would be applied to the school's physical buildings. All members of staff need to be aware of the possible misuses of on-line access and their responsibilities towards pupils. The guidelines for pupils are designed not only to ensure facilities are used responsibly but also that pupils use them safely, and staff should be particularly aware of issues surrounding the online safety of pupils, in particular:

- Use of messaging, mail and social media for cyber-bulllying and intimidation.
- Preventing access to inappropriate content
- Preventing on-line contact with inappropriate individuals
- Maintaining privacy and control of personal information

Any staff who have any concerns about using the Internet with pupils or their ability to monitor and guide pupils in their use of the Internet should seek advice from the Computing HOD or the ICT Manager *before* they undertake any Internet activity with pupils. If you require more details regarding the issues surrounding the use of IT and the Internet in schools, please speak to the IT Manager.

If you have concerns about a child as a result of their on-line activity, or feel they may be a victim or instigator of cyber-bullying, regardless of whether they are using school equipment, then you should use the usual pastoral systems we have in place in school to escalate the issue to the Head of Year, or Safeguarding Lead as appropriate. If you believe that a child has been viewing inappropriate content then you should report this to the IT Manager who will investigate and escalate the matter if required.

It is considered a professional requirement of staff that they have an understanding and awareness of the issues surrounding the use of IT and the internet with pupils. All staff are therefore expected to assist in the management of pupil access to IT by ensuring that any pupils under their supervision comply with this policy and the guidelines for pupils mentioned below.

Internet and network access for pupils should be viewed as a privilege and not a right. Pupils who fail to abide by the pupil acceptable use policy may be denied access to the Internet or to the school network for periods of time. Staff who supervise pupils' network use will be informed of the names of any pupils who are not allowed to use the Internet or network and are responsible for helping to enforce any restrictions.

Any member of staff who believes that anyone is misusing the IT facilities or breaching the terms of this policy should report any such incidents to the ICT Manager as soon as possible, or if there are significant associated issues regarding pupil behaviour to the appropriate line managers or pastoral leader.

It is likely that pupils may attempt to make use of 3G mobile phones to access social media sites such as Facebook or send each other texts or pictures. As these are not school devices, and they are not using the school wireless network, there is no technical way of monitoring

such use, but staff should be aware of the possibility that this may happen, and enforce the school mobile phone policy as appropriate.

Use of Social Media

It must be recognised that any views or opinions communicated using social media or e-mail may be seen as a corporate opinion of the school or LA, which has the same status as formal written correspondence. Any expression of a personal view about the school or LA using such media must therefore be clearly labelled to that effect.

Staff are advised that they should not use personal social media accounts on services such as Facebook or Twitter for one to one communication with pupils, parents or carers. One to one communication with pupils may be appropriate for some teaching and learning activities but it is vital that all such interactions are transparent and open to scrutiny at all times. Staff should not respond to friend requests from pupils and should avoid entering into online "friendships" with parents/carers or pupils as this could lead to professional relationships being compromised.

Staff to student digital communications relating to curriculum matters (such as handing in homework) can be done using school provided Office 365 or Google e-mail accounts which are regularly monitored by the IT support staff.

Staff should exercise appropriate discretion and be aware of the relevant professional standards to which they will be held when posting information on the internet that may come into the public domain. You are strongly advised to make use of the appropriate privacy settings offered by social media sites to limit access to your online presence as appropriate, to protect yourself online.

You must ensure that your online activity will not undermine your professional role. Your online activity, whether taking place inside or outside school, should not interfere with your work duties, should not bring the school or LA into disrepute, and must be in accordance with this policy and the Law.

Staff should not set up social media accounts relating to the school or their work at the school without first consulting with the IT Manager and the Web Manager. The school has official social media accounts on Twitter, Facebook and YouTube which are used to engage with students and the wider community. There are specific rules around their use outlined in the schools' Social Media Policy and staff wishing to use social media for school related purposes should use these official accounts only, and in accordance with the relevant school policies.

Data Protection and Legal Issues

You should be aware that misuse of computer systems is covered by Criminal Law and some activities may constitute an offence under the Computer Misuse Act and lead to criminal and/or disciplinary proceedings.

Users of the IT systems should note that all access is logged and can be traced to individual users and/or computers. Similarly e-mail and web traffic is monitored by the IT support staff. *E-mails into and out of school should not be regarded as secure or confidential*, *and should not be used for the transmission of confidential or personal information about students or colleagues*.

Web filtering is applied at the school level and this local filter is maintained by the IT Manager. It is designed to protect pupils and staff by filtering out web content that would be inappropriate to view in a school environment. If you come across an accessible web site or an line resource which you feel should be restricted, please contact the IT Manager. Similarly, if you wish to check on previous web activities of specific users, or wish to use a website or facility which is restricted by the filter and you believe is appropriate to use in school, speak to the IT Manager. Please be aware that it may not be possible to allow access to some sites which are blocked by the filter for technical or legal reasons and that allowing such access is at the discretion of the IT Manager.

The school has a legal obligation to comply with the requirements of the Data Protection Act and the Prevention of Terrorism Act, and to ensure that any usage of IT systems takes into account all relevant child protection legislation. In order to do this, information about pupils, (including photographs and video), and any data relating to colleagues, parents and other partners of the school stored on the school computers must be protected from unauthorised access. To comply with these requirements all staff should be aware of the following:

1. There are specific secure methods used by the school for transferring sensitive data such as pupil records in and out of our systems. **You must not remove from the school site any detailed personal data about pupils, parents or any other third party which we hold on our IT systems by copying it onto a memory stick or other media unless you have specific authorisation from the Headteacher and have been provided with an approved secure method of doing so by the IT Manager.**

2. **Consequently, you must not store any personal information about pupils or staff on a computer at home including any computer provided by the school.** Staff who need to work on this type of data at home who have been authorised by the Headteacher to do so will be issued with encrypted laptops or memory sticks by the IT Manager. Staff who wish to access such data from home computers should use the remote access facilities provided. Please see the IT Manager if you need any clarification on this point.

3. **Personal Data relating to third parties and covered by the requirements of the Data Protection Act can only be stored on the school computer network in certain specific locations, which are subject to appropriate security and auditing controls and will be**

defined by the IT Manager and made clear to all relevant staff. Copying such data to other areas of the system where the appropriate controls may not be in place is not permitted.

4. You must not tell your network password to anyone else, **and you should not write it down anywhere**. You must not allow anyone else to use your password to remotely access the network. If you believe that someone else is aware of your password you should inform the IT Manager immediately.

5. When accessing the school network remotely you must ensure that you completely log off the system before leaving the remote computer. You must not access the school network from public access computers, for example cybercafés.

6. You must not leave any computer which is logged into the school network using a staff account unattended at any time – either log off the machine or lock it.

7. You must not **under any circumstances** allow pupils to use a computer that you are logged on to, or allow pupils to log onto a computer intended for staff access only.

.

8. You must not give out names or personal information relating to other staff or pupils at the school on any public web sites or forums, or transfer such information to a third party, even to confirm that they are on roll at the school, unless it is a specific part of your job role to do so and the transfer complies with the requirements of our data protection registration.

9. If you wish to upload pupils' work to web sites or pass examples of work on to others not directly connected with the school you cannot do this without their permission and you must record that you have received this permission.

10. You should take care with the use of images of pupils. You should not circulate images of pupils (for example photos taken on trips or visits) on personal social media accounts. You should also avoid taking or storing photos of pupils on personal cameras, phones or computers: If you need to take pictures of pupils for official school purposes, use a school device, not your own personal one.

11. Pupils and/or their parents have a right to object to their pictures being used in any way except for school administration. The terms of the DPA apply to the photographs of pupils we store in the SIMS database. These can be used for administrative purposes within school, for example identification, pupil tracking and security, but not for any other purposes unrelated to the school, as this is not why the images were collected. If you are using photographs or video of pupils for publicity materials, news items or on the internet, anything in fact which is likely to circulate outside school, (and this includes images you may wish to put on the school website) you must tell pupils this beforehand and keep a record of the fact you have done so. We ask permission to use images and video on the school admission form and the pupil record in SIMS shows whether such permission has been granted. The school Web manager will not use images or video of any pupils if we do not have confirmation that such permission has been received.

12. You must observe copyright regulations with regard to any material you store on the school systems. Some material can be copied for personal use but not commercially, and conditions of use may specifically exclude schools: read any conditions of use or copyright statements carefully. Any material found on the school network which appears to breach the restrictions of our copyright licence will be deleted without notice. If you require further guidance on this point please speak to the Reprographics Manager, who will be able to clarify what material is covered by our licences.

13. You should not allow any other person access to your school e-mail account, including any other employee of the school or any pupil. You **must** use your school provided e-mail accounts for any school related business. This is in order to ensure transparency, that we have a full audit trail of any correspondence, allow us to have secure backups of all e-mails relating to school business, and to enable us to meet our obligations under the Freedom of Information and Prevention of Terrorism regulations. You must never use a private e-mail address to communicate with parents or students for any school related business.

Specific Policy Conditions

The following activities, whilst not an exhaustive list, are unacceptable and are **strictly prohibited** under the terms of this policy:

1. The access to or creation, transmission or publication of any offensive, racist, obscene or indecent images, sounds, data or other material which is inappropriate for viewing by children.

2. The creation, transmission or publication of any material which is designed or likely to cause offence, inconvenience or needless anxiety to a third party. *In particular the use of ICT facilities to intimidate bully or abuse another member of the school community.*

3. The creation, transmission or publication of defamatory material.

4. The receipt or transmission of material such that this material infringes the copyright of another person or infringes the conditions of the schools' Data Protection Registration or the general conditions of the Data Protection Acts.

5. The downloading and installation of any software on any computers linked to the Siddal Moor network without the prior consent of the ICT Manager.

6. Deliberate activities with any of the following characteristics or that by their nature would result in:

- wasting network resources, or the time of IT support staff
- corrupting or destroying other users data
- violating the privacy of other users
- disrupting the work of other users

- using the Internet in a way that denies service to other users (for example, by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading large files).
- continuing to use any item of software after being requested to cease its use because it is disrupting the correct functioning of the school's network or the Internet (for example, utilities designed to broadcast network- wide messages)
- the deliberate introduction of viruses or similar programs

7. Where the Internet is being used to access another network, such as the Rochdale Schools Intranet, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the Siddal Moor service and associated resources.

8. The transmission of unsolicited commercial or advertising material to other users of the network or any other network reachable via it.

9. Any use of the network that would bring the name of the school or Rochdale LA into disrepute.

10. The use of the service for any commercial purpose which is not directly related to the users' job function, ***including the use of on-line commerce sites for the private purchase of goods or services***.

11. The disclosure of any username or password required to access the service or the use of any such disclosed username or password to access the service or allow others access to the service.

12. Any attempt to facilitate unauthorised access to facilities, services, data or resources within the Siddal Moor Network or any other network or service directly accessible from it.

Staff Tablet Devices and iPads – Terms and Conditions of Use

Users of these devices must at all times use them in accordance with the principles of the school acceptable use policy. However, there are specific issues related to these wireless devices which users should be aware of:

- Some of these devices are configured to access the School SIMS system. This means that they may have access to sensitive data the use of which is governed by the Data Protection Act, and users of the devices should be conscious of this at all times.
- If the device is lost or mislaid, the loss **must be reported to the IT Manager as soon as possible**, so that the data on the device can be remotely wiped and access to the device blocked.
- If you have any reason to believe that the device has been subject to unauthorised access you must inform the IT Manager of this as soon as possible.
- Users should set a PIN access code and use it whenever appropriate.
- The devices are not to be used by any person not directly employed by Siddal Moor Sports College.
- **Staff Devices are not to be used by students under any circumstances.**
- Whilst users may install applications by setting up an appropriate Apple ID account, they should not change the basic configuration of the device or uninstall any applications installed by the school IT support staff.
- The devices are synchronised to a school computer running specialist configuration software. They should never be connected to computer running iTunes as this may cause the devices to be wiped and settings lost.
- They must not be used to store personal music or photo collections as the memory available is limited and this may inhibit the operation of other Apps required for school use.
- Staff are reminded that these devices are not secure or backed up regularly and should not be used for long term storage of critical files. Similarly, if they are used for taking video or still images of pupils for school purposes, these files should be transferred to the school network and deleted from the device as soon as is practicable.

Staff Laptop Computers – Terms and Conditions of Use

- Certain staff whose jobs may require one are allocated a laptop computer in order to assist with school work.
- The computer remains the property of the school. If you leave Siddal Moor or, in the opinion of the Headteacher, you are not making effective use of the machine and it would be more usefully employed with another colleague you must return it to the school along with any software, cases and accessories.
- The computer is for your personal use to assist you in carrying out your job function. **It should not be used by any other individuals or other members of your family for any purpose whatsoever.**
- You must not use the computer to do anything which would contravene the principles of the Siddal Moor Acceptable Use Policy.
- Your computer may be equipped with software which allows the programs run and web sites visited to be logged. When the computer is returned to school the IT Manager reserves the right to check these logs to ensure compliance with the Acceptable Use Policy.
- If you experience a failure or problem with your computer please see the IT Manager in the first instance, who will deal with any repairs.
- The computers come with a comprehensive software package, but you are free to install any additional software on your machine for which you have a valid licence. You must not install any software on the computer for which you do not hold a legitimate valid licence.
- The computers have anti-virus and firewall software installed which must not be removed. This software may prevent some other applications from working correctly, and we cannot guarantee that all software you may wish to install on the laptop will work.
- If you wish to use the computer on your home internet connection you may install any software or hardware required to do this but please note that we cannot provide technical support for home internet connections and these connections are entirely your responsibility.
- From time to time you will be required to bring the computer into school for checking and audit purposes and to allow software updates. You must bring your computer into school when requested to do so by the IT Manager.
- Computers are only insured under the school policy whilst on the school premises. Should the computer be lost or stolen whilst in your possession the school reserves the right to recover the full replacement value of the machine from you. It is your responsibility to ensure that the computer is adequately insured and you should therefore check with your insurance company that your home or personal insurance covers the machine whilst it is in your possession or left at your home, and arrange cover if this is not the case.

Siddal Moor ICT Acceptable Use Policy for Pupils (1)

- You must not tell anyone else your network username or password. You must not use anyone else's username or password to access the school network. This is to help protect your work, your privacy and your safety.
- If you think someone else knows your password you must tell your teacher at once so that it can be changed.
- If you find any damaged or broken equipment report it to your teacher at once and do not use it unless you are told it is safe to do so. You should take care to use the school computers carefully. If you cause any damage to school computers you will be billed for the repair cost and may be stopped from using them in the future.
- You must not install any programs onto a school computer or change the settings or configuration of any school device.
- When you have finished using a computer you must ensure that you log it off properly so that no other users can access your files.
- Files saved on the school network are not private – teachers and the IT staff can look at them. If files contain anything inappropriate or offensive they will be deleted, your parents may be notified and further action may be taken.
- If you have a school e-mail account, this is not private – teachers and the IT staff can look at your e-mails. It they contain anything inappropriate or offensive they will be deleted, your parents may be notified and the e-mail account will be deleted.
- We keep backups of the network and if you accidentally delete files we may be able to retrieve them, but it is your responsibility to make sure you keep backup copies of important files, such as coursework. Your teachers will help you with this.
- The network keeps a record of all your computer activity. We can tell when you used a computer, what you printed and which software you used.
- When you use the internet, your access is controlled by a web filter, this is used to protect you and you must not try to bypass it. We keep a log of all web sites that you visit and all internet searches that you carry out.

Siddal Moor ICT Acceptable Use Policy for Pupils (2)

- If we find you have tried to visit inappropriate sites we may remove your ability to access the internet and/or restrict your use of the school computers.
- Certain types of files are not allowed in your network folders. Shortcuts, programs, scripts and any files with inappropriate contents will be deleted without warning if found. You should not keep personal files which are nothing to do with your school work on the school system.
- You must not download or save any material which is copyright, and you are not allowed to use file sharing sites. You must always check with your teacher before using any material from the Internet in coursework.
- Our computers are provided for you to do school work and you should not use them for personal tasks such as your private e-mail, chat, texting, Facebook, or for playing games.
- The school will not use any of your work on the Internet or our web site, or give out any information about you, unless we have separate written permission from you.
- Under no circumstances should you attempt to view, or download any material which is considered to be unsuitable for children or is age restricted. This applies to any material of a violent, dangerous, or racist nature or which has inappropriate sexual content.
- If you accidentally find any material that you think is unsuitable for children or which you find offensive, tell your teacher immediately.
- If we find that the network has been used to bully or harass anyone we will take that very seriously. Anyone using our school network to do anything illegal will be reported to the Police.
- You must take responsibility for you use of the computers and the internet in school.

Remember:

a) online actions and can have offline consequences
b) people you meet on the internet are not always who they say they are
c) to think about your own safety and privacy at all times.

www.thinkuknow.co.uk