IT Acceptable Use Policy
For Staff and Code of Conduct Agreement

Overview
The main points of this policy can be summarised in the key sentences below. Users are **NOT permitted** to undertake any of the following actions:

1. Logging on to the network with another user's account
2. Using computers to send offensive or harassing material to others, either internal or external to the school.
3. Altering the settings of the computers or making other changes which render them unusable by others
4. Tampering physically with the equipment
5. Attempting to access unauthorized areas of the network
6. Accessing inappropriate web sites or trying to circumvent the school's systems. This includes the use of proxy servers for this purpose.
7. Attempting to spread viruses via the network
8. Using school computers for any form of illegal activity, including software and music piracy.

Breach of the acceptable use policy may result in disciplinary action being taken.

Computer Facilities

Rules
The following rules apply to all computers which are provided by the school or connected to the school network. It also applies to devices which are used whilst on school premises: i.e. mobile devices that access the internet via 3G modems.

General Conduct and Use
Any damage to computers, furniture or fitments should be reported to a member of ICT Support. The same applies to any apparent malfunction of equipment.

Use of the Network
1. When logging on to the network, staff must always use their own user identification and password.
2. Any member of staff who identifies a security problem on The Oaktree School network must notify ICT Support immediately via email to james@peersict.co.uk detailing the problem.
3. Staff must never divulge their passwords or write them down unless required to do so by ICT Support for support purposes and then they should change them afterwards. Any member of staff who suspects that their password has been compromised, accidentally or otherwise, should change their password without delay.
4. Staff must not use the computer network to gain unauthorized access to any other computer network.

5. Staff must not attempt to spread computer viruses.
6. Staff must understand that the information they hold on the network is not private.
7. Before leaving a computer, staff must always log off the network or lock their terminal and check that this procedure is completed.
8. Staff may leave computers on to access the remote server when working from home (log off and turn screen off)

Data Protection

Data protection is the responsibility of all members of staff. To this end -

1. Staff must not disclose to a third party the personal details of another member of staff, a pupil or a pupil's family. When sending emails, staff should ensure the anonymity of addressees by making use of the BCC (blind carbon copy) functionality when addressing emails.
2. Staff must ensure that they do not retain copies of the personal details of another member of staff, a pupil or a pupil's family on their laptops. If staff require pupil lists for carrying out their duties then the information should be removed as soon as it is no longer needed
3. Staff must ensure that their laptop are kept secure when away from school and report any loss of devices or data immediately.
4. Do not disclose sensitive data to third parties without authorisation from either the ICT manager or the Data Controller
5. Staff should also refer to the School Data Protection Policy
6. USB stick are not to be used due to the risk of them spreading viruses

Internet and E-mail

Email Rules

1. Staff must not send electronic communications which are impolite, indecent, abusive, discriminatory, racist or in any way intended to make the recipient feel uncomfortable.
2. Staff must not make inappropriate use of the email system and address book, such as sending bulk emails, chain emails or for personal marketing purposes.
3. Staff must not use their email account to send or exchange material of an undesirable or illegal nature.
4. Staff must not open emails from unknown senders due to the risk of viruses.

Internet Rules

Whilst the school internet facilities exist principally for enhancing the educational purposes of the school, staff may make personal use of the internet in their own time provided this doesn't detrimentally affect the school's primary function. Staff should also be aware that all internet usage is logged.

1. Staff must not breach another person's copyright in any material.
2. Staff must not attempt to access inappropriate websites using the school network and should be aware that all websites accessed are logged.
3. Staff must not upload or download any unauthorised software or attempt to run that software. In particular hacking, encryption and other system tools are expressly forbidden.
4. Staff must not engage in activities that are prohibited under UK Law. Thus the transmission of material subject to copyright or protected by trade secret is forbidden.

Software

1. All Oaktree School installed software is subject to change and may be updated or removed at the school's discretion when deemed necessary.
2. Staff should not remove or uninstall any of the School installed software without consultation with ICT Support.
3. Staff may install software on classroom machines or laptops but must consult with ICT Support in the first instance to reduce the chance of conflicts with existing software.

Laptops & Personal Data Appliances

Staff are provided with a school-owned device for the better performance of their teaching and/or administrative duties. ICT Support will work to ensure that the device provided is suitable for the needs of the member of staff and will be available to assist with maintenance or training in the use of the device. By accepting the provision of a school-owned device, staff agree to the above policy and in addition the following rules:

Rules

Connection to the network

1. In order to help keep the network secure, safe and virus free, connection to the Oaktree School network of any unauthorized device is strictly forbidden. The only devices that can connect to the Oaktree School network are those which have been authorised by ICT Support.
2. A device should be connected to the school network at least once a week to ensure the any necessary updates can take place and that the antivirus software is up-to-date.
3. Under no circumstances should computers, printers or other devices be detached from the network to make way for a device.
4. Unauthorised devices must not be connected to the network.

Monitoring

4. Devices are monitored by ICT Support to ensure they are running effectively. This will also record any new software that has been installed and when the latest updates occurred.

Damage or loss

1. The school cannot accept responsibility for any damage caused, to devices or their contents (files, folders etc.) by inappropriate use.
2. Any damage to the device, whether accidental or otherwise, should be reported to ICT Support as soon as possible.
3. Staff are provided with a device protection to protect the device when in transit. Please ensure peripherals, such as a mouse has been unplugged before putting the device in the bag as failure to do so can damage the sockets on the device.
4. A charge may be incurred if the device or its peripherals are damaged by improper use. A charge may also be incurred to cover insurance excess if the device is lost or stolen due to insufficient security of the device.
5. Whilst in transit, devices must be stored out of site, preferably in the boot of the car. If the car is left unattended then the device MUST be stored in the boot, out of site. Failure to do so will negate the school insurance cover and the member of staff may be liable for the cost of a replacement device.
6. At home, devices must also be stored out of site, preferably in a locked draw or cupboard, when not in use.

Licensing and copyright

1. It is the responsibility of the owner to ensure that they have a licence for any additionally installed software over and above that which is already provided with the device.
2. Staff are responsible for ensuring that the copyright of media files (music, images and video) is not breached by illegal copying of such files.
3. Staff are responsible for the material that exists on or is accessed via their device.

CODE OF CONDUCT

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email/internet/Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will ensure that all electronic communications are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission of the IT Team.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and /or staff will only be taken, stored and used for professional purposes in line with the above policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without the permission of the parent/carer, member of staff or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will report any incidents of concern regarding children's safety to the Headteacher or Child Protection Officer.
- I will ensure that electronic communications with children including email, IM and social networking are never entered into.
- I will use social networking sites in a professional manner and in accordance with the schools Online-safety Policy.
- I will support the school's Online-safety policy and help children to be safe and responsible in their use of ICT and related technologies. I will promote Online-safety with children in my care and will help them to develop a responsible attitude to system use, communications and publishing.

I have read this IT Acceptable Use Policy, Social Networking Policy, Data Protection Policy and Online-safety Policy and I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name……..……(printed)

Job Title ……

Signature ……..