Acceptable Use of ICT Policy

Staff Policy

OASTLERS SCHOOL

Safe Secure Successful

Oastlers School

Policy Document

Contents

Introduction

The use of the latest technology is actively encouraged at Oastlers School. With this comes a responsibility to protect all users and the school from abuse of the system.
All staff therefore, must adhere to the policy set out below. This policy covers all computers, laptops and electronic devices (such as iPod touches, music equipment, games equipment, cameras and iPads) within the school, irrespective of who owns the device.

It is unlikely that any set of rules can cover all circumstances that may arise. The following set of rules is not intended to be a complete list of all possible “offences”. The emphasis is on outlining standards of performance and behaviour which are expected of Oastlers Staff, any users of Oastlers ICT Services.

1. Access

As staff at Oastlers School, I have access to the following ICT facilities:
1.01 Computers, laptops and specialist equipment throughout the school
1.02 Smartboards and visualisers in teaching rooms
1.03 A secure username and password for logging into:
1.03.1 School computer systems
1.03.2 SIMS Learning Gateway/Blue Sky/Sleuth
1.04 An accredited, filtered Internet connection from any Computers, Laptop or Mobile Device in school
1.05 An allowance of personal user space on the school network.
1.07 Internal and external remote access to the school network VIA a Secure Access Portal to store and share learning resources.
1.08 A personal @oastlers.co.uk email account with 10GB of email storage space.
1.09 Access to network printers. All staff have access codes/Cards for the printers.
1.10 Access to resources such as visualisers, digital cameras, camcorders, games equipment and microphones.
1.11 Access to the following software for home computer use:
1.11.1 Microsoft Office Suite
1.11.2 Serif Suite
1.11.3 Smart Notebook 11
1.11.4 Sophos Antivirus
1.12 Access to the School Management Information Systems (SIMS.net) as appropriate to role in school.
1.13 If I bring in my own ICT equipment I may be able to see the Network Manager or ICT support personnel to connect it to the school wireless guest network.
1. 14 Blue Sky Staff CPD
1. 15 Sleuth Staff Behaviour management and reporting system
1. 16 Curriculum specific softwares’

2. E-Safety

2.01 I will ensure that I am aware of e-safety issues affecting staff, parents/carers and learners. Read and comply with guidance. Visit our e-safety Policy and guidance on the school website. Keep up-to-date through our ICT Lead, CEOP and SID (Safer Internet Day) or other CPD events.2.02 Staff will remind learner of key e-safety messages such as ‘never give out personal details online’, be aware of your digital footprint

2.03 I will report any accidental access to inappropriate material to the ICT Network Manager immediately

2.04 I will report any inappropriate websites to the ICT Network Manager

2.05 Staff will be vigilant when searching for images and asking learners to search for images and encourage use of creative commons and royalty free image sites

2.06 If a learner accesses inappropriate material staff will report it following the correct procedures

2.07 If I suspect a Child Protection issue I will report it to the named person for child protection and follow the correct procedures.

2.08 I will always be myself and will not pretend to be anyone or anything that I am not on the Internet.

2.09 I will always protect the online reputation of the school and act in a digitally professional way

3. Computer Security

3.01 I will use computers with care and leave ICT equipment as I found it. I will not tamper with computer systems or devices (*e.g.* printers and projectors) and their cabling, internal parts or casings

3.02 If I notice that ICT equipment or software is damaged or not working correctly, I will report it via the ICT Network Manager straight away

3.03 I will use the ICT Service Desk Portal to report ICT related issues whenever possible.

3.04 I will never try to bypass security features or systems in place on the network, or try to access resources or a user account that I do not have permission for (hacking).

3.05 I will never attempt to install software on Computers, Notebooks, Mobile Devices or ICT Equipment myself and will request a software change through the ICT Service Desk Portal.

3.06 I will always keep any of my user account credentials secure and not tell them to anyone else or share them with anyone else.

3.07 I understand that my logon gives me access to systems and information that other staff are not entitled to access and I will not under any circumstances allow anyone else access to a computer under my logon credentials

3.08 I will not attempt to go beyond my authorised access. This includes attempting to log on as another person, sending emails whilst pretending to be another person or accessing another person’s files. If I find that I do have access to an area that I know I should not have access to, I will inform the ICT Network Manager immediately.

3.09 If I think someone else has obtained my logon details, I will report it to the ICT Network Manager as soon as possible to get my logon credentials changed
3.10 I will never knowingly bring a computer virus, spyware or malware into school.
3.11 If I suspect a school computer or a removable storage device that I am using contains a virus, spyware or other malware, I will report this to the ICT Network Manager.
3.12 I will not attempt to connect to another user's laptop or device while at school. I am not permitted to establish my own computer network
3.13 I will take care if I eat or drink whilst using ICT equipment
3.14 I will not reply to spam emails as this will result in more spam. I will delete all spam emails.
3.15 If I lose or misplace any portable ICT equipment I will inform ICT Network Manager immediately.
3.16 I will not 'jailbreak' a school iPad, iPhone or iPod touch
3.17 I will not share my personal details with any learner at any time.

4. Inappropriate Behaviour

4.01 I will not store, download or distribute music, video or image files on my personal user space unless they are copyright free media files related to school work
4.02 I will not send or post defamatory or malicious information about a person or about school
4.03 I will not post or send private information about another person
4.04 I understand that bullying of another person either by email, online or via text message will be treated with the highest severity
4.05 I will not use the internet for gambling
4.06 I will not access material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people
4.07 If I am planning any activity which might risk breaking the ICT Acceptable Use Policy (*e.g.* research into terrorism for a legitimate project), I will inform the ICT Network Manager to gain permission.
4.08 If I mistakenly access material that is profane or obscene, I will inform my line manager immediately or I may be held responsible
4.09 I will not attempt to bypass Oastlers School Proxy.
4.10 I will not take a photo or video of a learner or member of staff without their permission
4.11 I will not load photos or videos of staff and learners to websites or social networking sites. I will refer this job to ICT Network Manager (e.g. if I wish to put pictures from an event or trip on the Web Site).
4.12 I will not behave in a way which could bring the school and its community into disrepute. This includes posting comments via social media that may harm the reputation, or feelings, of colleagues and the school in general.

5. Monitoring

5.01 I understand that all Internet and email usage will be logged and this information could be made available to my line manager on request
5.02 I understand that all files and emails on the system are the property of the school. As such, system administrators have the right to access them if required
5.03 I will not assume that any email sent on the internet is secure. I will use the school email signature with a disclaimer
5.04 I understand that all network access, web browsing and emails on the school systems and laptops are logged and may be routinely monitored on any computer screen without a person's knowledge.

6. Best Practice

6.01 I will not use school printing facilities to print none-work related materials unless given explicit permission to do so by the Headteacher.
6.02 I will only print out work that I need as a paper copy – where possible I will use school systems such as email, shared folders and school encrypted media to share information electronically.
6.03 I will follow the school's procedure and use the ICT Services Desk Portal to log an incident and request (unless an emergency) for myself and/or learners.
6.04 I will report it on the ICT Service Desk Portal if I believe a printer is not working or out of toner, or not printing double-sided.
6.05 I understand that my @oastlers.co.uk e-mail is a work e-mail account, and as such will be used for professional purposes. My personal or home email systems will never be used for school business
6.06 I will only use the approved, secure @oastlers.co.uk e-mail system for any school communication
6.07 I will only open attachments or download files from trusted sources
6.08 I will not view, download or distribute material that could be considered offensive or pornographic
6.09 I will obtain the school cameras from the ICT Network Manager to photograph and video trips and relevant events (I will not use my own cameras or phone without prior arrangement).
6.10 I will pass relevant photographs and videos taken on to the ICT Network Manager for storage on the school network (I will not keep images and videos of learners in my personal user space or on my own devices, and will ensure they are on a shared networking area).
6.11 I will save work regularly using sensible file names
6.12 I will organise my files in a sensible manner and tidy my user space and shared resource areas regularly
6.13 I will ensure that I regularly back up any work that is not saved onto the school network
6.14 I will observe health and safety guidelines where possible when using ICT equipment

6.15 I will leave my computer and the surrounding area clean and tidy
6.16 When I leave school permanently, I will ensure that I save any files I wish to take with me as my account will be deleted
6.17 I will only empty my recycle bin when I am certain I no longer need the files
6.18 I will seek advice from ICT Network Manager or Line Manager before ordering any ICT equipment for my department.
6.19 I will not print on glossy paper, card or acetate on laser printers.
6.20 I will comply with copyright law and acknowledge and credit sources for any copyrighted and published work

7. Data Protection

7.01 I will not share data protected information (including school images) with third party organisations without seeking advice first
7.02 I will use an encrypted storage device (such as a USB drive encrypted using Truecrypt or other similar software) to transfer data protected files between home and school. Alternatively, I will remote access rather than move the files physically.
7.03 If I am preparing a document that contains data protected information I will ensure that the document template I use has the appropriate protective marking (*eg* confidential, protectively marked).
7.04 I will ensure that I am aware of data protection issues and understand what is considered to be 'personal data'.
7.05 I will not display sensitive information or 'personal data' on a public display or projected image (*e.g. a* smartboard). This includes learner data in SIMS.net.
7.06 I will never leave a computer logged on and unattended for even a short space of time. I will log off or lock the workstation. I understand that failure to do this may result in a breach of the Data Protection Act and leave 'personal data' unprotected.
7.07 I will ensure that any remote connection session that I have to a school computer is logged off when I have finished and kept secure from other computer users.
7.08 I will not take sensitive data off site without relevant approval

8. Social Networking

8.01 Staff will **not** communicate with learners through social networking sites at any time
8.02 I will ensure that any personal social networking accounts that I have do not compromise the professional reputation of the school and are not used or accessed in School Working hours.
8.03 If I have control over a school Twitter account I will:
8.03.1 Keep it as a protected account at all times
8.03.2 Change the Password regularly
8.03.3 Maintain the highest standards of professionalism
8.03.4 Only follow professional educational organisations, other organisations as deemed appropriate
8.03.5 Inform a Senior School Leader or ICT Network Manager straight away if I suspect I have lost the password or advice with that account on it

8.03.6 Never use the account to send Direct Messages to anyone
8.04 I will **not** create a bogus social networking account or site that is associated with a member of staff, learner or the school.
8.05 If I become aware of misuse of Social Networking accounts or sites that are associated with a member of staff, learners or the school, I will inform the Senior School Leadership or ICT Network Manager immediately.
8.06 I recognise that as an organisation, we do not use social networking sites to communicate with learners, staff and parents/carers (with the exception of any official Social Media accounts).

9. Legal

9.01 Much of the data, information and IT systems within Oastlers School are covered by the statuary legislation including

- The Freedom of Information Act 2000
- The Data Protection Act 1998
- The Copyright Designs and Patents Act 1988
- The Computer Misuse Act 1990
- Environment Information Regulations Act 2004
- Privacy and Electronic Communications Regulations 2011

10. Sanctions

10.01 I understand that failure to comply with this Policy may lead to disciplinary action.

11. Staff, Governor and Visitor Agreement

11.01 I understand that the Acceptable Use Agreement is only a summary of the ICT Acceptable Use Policy (Staff) and that by signing the Acceptable Use Agreement i will adhere to the Acceptable Use Policy (Staff).

Oastlers School

Policy Document

Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Oastlers ICT Network Manager

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher 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 will ensure that all electronic communications with staff are compatible with my professional role.
- I will **not** give out my own personal details, such as mobile phone number and personal e-mail address, to learners.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) 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 or accessed remotely when authorised by the Headteacher or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the ICT Network Manager
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of learners or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the 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 support and promote the school's e-Safety and Data Security policies and help learner to be safe and responsible in their use of ICT and related technologies.
- Failure to adhere to the guiding principles of this policy may lead to disciplinary procedures.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….…………………….………… Date ……………………

Full Name ……………………………….......................................(printed)

Job title ……………………………………………………………………