Staff ICT and Internet Acceptable Use Policy Agreement

We encourage you to use the School's ICT resources responsibly. Should you have any questions regarding this Acceptable Use Policy, you should contact the Director of IT.

I hereby acknowledge that I have read and understood the Woldingham School Staff ICT and Internet Acceptable Use Policy. I agree to abide by this policy at all times when using School ICT. I understand that if I violate this Acceptable Use Policy Agreement, I may face legal or disciplinary action according to applicable law or School policy.

Staff Name (printed): _____

Signature: _____

Date: _____

When completed, please return this Staff ICT and Internet Acceptable Use Policy Agreement to:

HR Office
Woldingham School
Marden Park
Woldingham
Surrey
CR3 7YA

The School's Staff Information Communications Technology [ICT] and Internet Acceptable Use Policy is attached

STAFF INFORMATION COMMUNICATIONS TECHNOLOGY [ICT] AND INTERNET ACCEPTABLE USE POLICY [AUP]

---

1. Purpose

1.1. This policy outlines acceptable and unacceptable use of Woldingham School's Information Communications Technology [ICT] resources. It includes information on general security, health and safety, the use of equipment, access to resources including the Internet, storage of data, the use of communication tools and support. Use of any ICT services is subject to the conditions given in this document.

2. Introduction

2.1. ICT provides Woldingham School with essential tools to support the delivery of Teaching and Learning, whole School administration, marketing of the School and communications both within and outside of the School.

2.2. Since the range and availability of ICT resources within the School changes frequently, this policy provides general requirements for acceptable use of all programs, services and resources currently in use and those that may be provided in the future.

2.3. Each member of staff is required to read this ICT policy and sign the Staff ICT and Internet Acceptable Use Policy Agreement to gain access to the School's ICT resources.

2.4. For the purpose of this document the following definitions apply:

2.4.1. **Acceptable Use of ICT Resources -** The types of activities that are considered to be acceptable use of the School ICT resources include:

- Participating in or creating resources for Teaching and Learning.
- Communicating with School communities to enhance and support Teaching and Learning.
- Communicating with third parties relating to School business matters.
- Acquiring or sharing information necessary or related to the Teaching and Learning; and
- Essential personal use as agreed with Heads of Year, Heads of Department, SLT or the Head.

2.4.2. Unacceptable Use of ICT Resources – The types of activities that are considered to be unacceptable use of the School ICT resources are those that do not adhere to any other School rule, School policy or the School Aims and Principles. This includes, but is not limited to, the following:

- Illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and tampering with any of the ICT monitoring or control systems (e.g. spreading computer viruses).
- Capture, storage and broadcasting of images without the prior permission of those featuring in the images.
- Excessive personal use of the Internet. The School allows limited personal use outside of the core School working hours for communication with family and friends, independent learning, and public service.
- The School prohibits ICT use for mass unsolicited mailings, access for unauthorised users to use the School's resources or network facilities, access to pornographic sites, gaming, using torrent sync and share services, sharing of computing resources for profit (e.g. BitCoin mining) and the dissemination of chain letters.
- Staff may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to the School or another individual without permission from the Director of IT.

3. Data Protection

3.1. Woldingham School takes its responsibilities for personal data very seriously and has policy in place to ensure compliance with the Data Protection Act 2018 incorporating the General Data Protection Regulations [GDPR].

3.2. The data collected during an employee's normal duties may contain data that is defined by the Data Protection Act 2018 as 'special category' data. This is the most sensitive category of data and as such it is essential that every care is taken to keep the data secure.

3.3. If there is any possibility that data has been lost then it must be reported immediately to the Privacy Officer (privacy@woldinghamschool.co.uk) for investigation. Any confirmed loss of special category data is reportable to the Information Commissioner's Office and may result in an external investigation.

3.4. All staff involved in collecting and processing any data during their normal duties must ensure they have read, understand and operate according to the school's Data Protection Policy. They must also be familiar with the school's Privacy Notice to ensure any processing required that is not covered by the Privacy Notice is reported to the Privacy Officer (privacy@woldinghamschool.co.uk).

4. ICT Safeguarding Policy

4.1 Staff should act in accordance with Safeguarding Children and Child Protection policy and all related documents issued to all staff as part of their Safeguarding Induction training that offer specific guidance on use of electronic communication. For further information contact the School's Designated Safeguarding Lead.

4.2 As a general rule, staff should not use their personal mobile devices or email to contact students or parents; your school email account, school telephone or a school mobile should always be used. However, if there is a particular situation that necessitates using personal devices or email accounts, the following examples of good practice should be adopted:

4.2.1 If you find it absolutely unavoidable to use personal email account, copy your line manager into the message. Use a School issued mobile phone to communicate with students or parents. If you need to use your personal mobile, for example on an overseas trip, clear this first with Deputy Head People, the Designated Safeguarding Lead or Deputy DSLs. In the interests of complete transparency, you are advised to copy your line manager into any texts which are sent from a personal mobile and do not store parents' or students' numbers on a personal device. Staff must ensure that pupils do not store their personal mobile number on their own devices. Staff must not use their personal mobile phone to make calls to parents (unless in an emergency).

4.2.2 School cameras to record images of students, not personal mobiles or cameras. If it is necessary to take pictures on personal cameras, permission from the DSL must be sought in advance, the images should be downloaded onto the School network as soon as practicable and then deleted from the personal camera. NB: photographic/video images may not be taken on a personal mobile. Staff must ensure that pupils are not using their personal devices to film or photograph staff.

5 Monitoring and Filtering

5.1 The School reserves the right to monitor any ICT activity occurring on the School network. In addition, the School employs content filtering software to limit access to certain sites on the Internet and monitoring software to record breeches of this ICT AUP and other School policies. If the School uncovers activities which do not comply with this policy, applicable law or other School policies, retrieved records of any computer activity may be used to document wrongful use and disciplinary action may be taken.

5.2 Content filtering systems are in place to ensure that the School is taking all reasonable measures to protect users from inappropriate content and also to protect the School from possible legal issues, relating to the storage of illegal files or material, when resources are accessed on the Internet. The filtering systems are reviewed regularly and updated to ensure that the highest possible level of protection is maintained. Since no content filtering system can be 100% effective, any user must report any viewed material that concerns them or is thought to be inappropriate to their Line Manager or the Director of IT. The filtering system will then be updated to prevent re-occurrences.

5.3 All access to the Internet is logged and any repeated attempts to access un-acceptable material or attempts to by-pass the content filtering systems will be investigated and disciplinary action taken as appropriate.

5.4 The monitoring systems are used mainly to provide warnings of potential safeguarding issues and abuse of the school ICT resources. The way these systems work can involve capturing an image of the computer screen when it detects a potential issue. This means anything displayed on the screen at that time may be captured. A screen capture is triggered by the appearance or typing of inappropriate content as defined by SLT.

5.5 Any incidents recorded by the screen capture system are monitored by a DSL and will be investigated and disciplinary action may be taken.

6 Security

6.1 For security purposes, where access to ICT resources is controlled by a username and password, staff must not share their network account or password information with another person or leave their accounts logged on at an unattended unlocked device.

6.2 ICT accounts are to be used only by the assigned user of the account for authorised purposes. Attempting to obtain another account password is strictly prohibited.

6.3 Passwords must be chosen that are considered 'strong' i.e, at least 8 characters including numeric and non-alpha (e.g. *&%$£) characters, and must never be written down.

6.4 A user must contact the IT Operations Manager to obtain a password reset if they have any reason to believe that any unauthorised person has knowledge of their password. Users must take all necessary precautions to prevent unauthorised access to Internet services. Guidance on setting a strong password can be obtained from the IT Operations Manager.

6.5 Laptops must be password protected.

6.6 To protect the School's ICT resources there are various security systems in place, in addition to network accounts, to prevent unauthorised access to the School's resources from the Internet and to detect and prevent infection from computer viruses. Staff must not attempt to change or remove any of these security systems.

6.7 The School has an open Bring Your Own Device approach via a wireless network which has various security and filtering systems in place to safe guard users. Any staff using their own devices on the wireless network do so subject to this and all other School policies.

6.8 Permission is required for the use of any equipment not owned by the School which requires a physical connection to the School network. Please contact the IT Operations Manager check for compatibility / correct operation on the School network and necessary security checks. Unauthorised devices may not be used on the School network.

6.9 Staff should never disclose personal information or contact information such as phone numbers and home/school address when accessing resources via the Internet. Do not use your School email details to register on any web sites or to register to receive regular emails. If you are concerned about the number or type of emails received or are worried you have disclosed your personal details then please talk to the Director of IT or the IT Operations Manager immediately.

7 Use of Communication Systems

7.1 When using any ICT resources that allow communication with other members of the School community or people outside of the School, it is vital that care is taken when composing the content of any message. The content of all messages must adhere to all other School rules and School policies. If you are in any doubt then consult another member of staff before sending the message. A good test is: would you be happy to see your message displayed next to the School logo on a notice board? If not, then the message probably should not be sent.

7.2 If using ICT resources on the Internet to communicate then only enter into a conversation with people whom you know and can confirm their identity. If anyone you do not know attempts to contact you via any method over the Internet then immediately close the program and report the site to the IT team.

7.3 E-mail

7.3.1 The School e-mail facility is provided for School business purposes only during established working hours. Staff should not to use e-mail for non-work related matters and should never use the e-mail system for the blanket mailing of any personal message either to e-mail Groups or across the School.

7.3.2 The School standard e-mail signature format must be enabled on at least all new e-mails. The use of the full signature is optional on replies. Please contact the IT Team for details and a template for the School Standard e-mail signature.

7.4 Telephones

7.4.1 Employees may make private use of the School's telephone system in cases of personal emergency only. Personal administrative calls are not to be made using the School's system.

7.5 Mobile phones

7.5.1 Students are not permitted to use personal Mobile phones during the School day (except in bedrooms, common rooms or Sixth Form coffee bar) or during any other School trip or activity without permission from a member of staff. The School expects staff to follow the same guidelines. Phones should be set to silent or vibrate only mode.

7.5.2 Staff personal mobile devices should not be used or left out/lying around except in department offices or staff common rooms. Under no circumstances should staff use mobile phones in the classroom for personal use.

7.5.3 Staff must have mobile devices password protected.

7.5.4 Staff must not use their personal mobile phone to make calls to parents (unless in an emergency). *

7.5.5 Staff must ensure that pupils do not have access to their personal mobile number.

7.5.6 Staff must ensure that pupils are not using their personal devices to film or photograph staff.

7.6 Social Networking Sites

7.6.1 The School uses various social networking sites and tools as part of the marketing of School activities. Where directed by a member of the SLT staff can access and place 'approved' messages on social networking sites.

7.6.2 The use of social networking sites for personal reasons is not permitted during the employee's core hours.

7.6.3 Employees using social networking sites for personal reasons[1] must ensure that, if adding information, they do not include reference to the School. The only exception is the sharing of information already published by one of the School official social media accounts. Failure to comply with this policy will be treated as a serious breach of the rules and may result in disciplinary action being taken.

7.6.4 Staff must not communicate with students via social media

7.6.5 Staff should not be 'friends', 'contacts', 'followers' etc. with students via any social media.

8 Electrical Safety

8.1 When using ICT resources it is very important to be aware of some basic electrical safety guidelines.

8.2 All ICT equipment owned by Woldingham School is regularly checked as per the Health and Safety policy for electrical safety. Certain types of electrical equipment owned by staff (and pupils) that are used in School are also subject to these electrical safety checks, please contact the Estates Manager for advice.

8.3 Whilst charging or using electronic equipment, heat is generated in both the power adapter and the device. To avoid overheating always ensure that the equipment and charger are placed on a suitable hard surface such as a desk and never on anything soft such as cushions, bed coverings or the carpets. Failure to do this could result in a fire.

8.4 If the equipment is not operating correctly, e.g. strange noises or sparks from the power adapter or device, or there is a burning smell then immediately switch the equipment off at the plug and report it to the IT team. Do not use the equipment again until told it is safe to do so.

9 Health and Safety

9.1 When using any ICT equipment you must take regular breaks to move around. You must ensure that the equipment is, wherever possible, located on a flat hard surface with plenty of room around it to work. Any cables being used should be sensibly positioned so they do not form trip hazards. The lighting and heat of the room should be adjusted to a comfortable level.

9.2 If at any time while using ICT equipment you experience headaches, tiredness or other muscular pains or spasms you must take a break immediately. If you regularly experience any of these symptoms then please make an appointment to discuss this with the Health Centre and inform the Director of IT.

[1] This excludes business sites (e.g. Linkedin)

10 Copyright

10.1 The majority of ICT resources available, both within the School and on the Internet, are copyrighted and as such cannot be downloaded and used without the prior permission of the resource creator. Under UK law, copyright material published on the internet will generally be protected.

10.2 Many websites will include a copyright statement setting out exactly the way in which resources on the site may be used. When using websites in School, staff must look for copyright information, to clearly identify the given permission to make a copy of the resource.

10.3 If permitted uses of the resource are unclear, it may be necessary to seek permissions directly from the owner of the website. Unless express permission is given, only a download and/or print of a single copy of a webpage should be made under fair dealing provisions. In all cases, copies should be acknowledged as far as is practicable.

10.4 Many online resources may have been published illegally without the permission of the copyright owners. Any subsequent use of the materials, such as printing, or copying and pasting, may also be illegal and could result in criminal proceedings.

10.5 The School ICT facilities must only be used with resources that are not subject to copyrighting. Any infringement of copyright agreements may result in disciplinary action and possibly criminal proceedings.

11 Storage of Data (see also data protection policy)

11.1 For every authorised user of the School ICT systems a secure personal storage area and access to numerous shared storage areas is provided. These areas are protected by various security systems and backup copies are made of the data every night. Access to these areas is possible from away from the School network so authorised users must store their data on these storage areas to ensure it is protected and recoverable in the event of any problems resulting in the loss of files.

11.2 The use of any non-School storage areas or removable media to move files around carries a risk of unauthorised access to the content and increased risk of unrecoverable data loss.

11.3 Removable media should only be used to transfer files when there is no other option and never for transferring any files of a confidential nature.

*Addendum – Changes in AUP during Covid 19

*Please note the change below (7.5.4) is time bound and subject to periodic review. This is intended purely as a means of facilitating communication with parents whilst the school is operating in accordance with DfE Guidance***.**

7.5.4 Staff during the closure of the school site, may contact parents using their personal phone. However, they should withhold their number when contacting the parent and keep a log of the call detailing: the time, duration and content of the call.

- In addition, whilst facilitating the ongoing meaningful teaching and learning of students, staff must follow the Remote Online Learning Policy created for the period whilst the school is operating in accordance with DFE guidance.