Wessex Schools Training Partnership

WSTP Acceptable User Policy

2021/22

Overview and Purpose

The purpose of this policy is to ensure that all trainees following an ITT programme at Wessex Schools Training Partnership (WSTP) are informed about appropriate procedures, laws and the risks associated with computer systems, email and internet access. It is not the WSTP's intention to impose unreasonable restrictions.

The protocols described herein are designed to protect users and to ensure that the WSTP and its partnership schools operate legally whilst at the same time avoiding damaging actions by hackers and others intent on causing harm. Inappropriate use of the network could result in virus attacks, data being compromised, and may also have legal ramifications for the individual(s) involved.

All computer related hardware and software, operating systems, storage media, network accounts, email and access to the Internet, Intranet, Extranet, WWW browsing and FTP are licensed to, and will remain the property of WSTP. These systems are only to be used to serve the educational and administrative purposes of WSTP.

Effective security will require the cooperation and support of all users. It will be the responsibility of every computer user to be familiar with these guidelines and to conduct their ICT activities within WSTP and its partnership schools in accordance with this policy.

Scope

This policy covers all equipment that is owned or leased by WSTP and all partnership schools of the WSTP; and applies to: - trainees, employees, students, contractors, consultants, and visitors.

General Use & Ownership

1. Whilst a trainee of the WSTP, all users must abide by the Data Protection Act (1998) and the Data Protection Regulation (2018), The Computer Misuse Act (1990) and offer any assistance required under the Regulation of Investigatory Powers Act (2000).

2. All WSTP trainees should ensure that confidential pupil data is stored in line with the relevant WSTP partnership school procedures. If in doubt, check with appropriate IT Manager.

3. While the WSTP aims to provide users with a reasonable level of privacy, users must be aware that the data they create on the systems remains the property of the WSTP or the WSTP partnership school. Because of the need to protect the network, management cannot guarantee the confidentiality of information stored within, transmitted over or on any peripheral device on the network.

4. WSTP trainees are responsible for exercising good judgment regarding the reasonableness of personal use. In the absence of such policies, employees should consult their mentor or WSTP School Rep.

5. For security and network maintenance purposes, authorised individuals employed by the school may monitor equipment, systems, and network traffic at any time.

6. Personal laptops, cameras, telephones, wireless networks, games consoles and other electronic equipment must not be connected directly to the WSTP or any WSTP partnership school network without the express permission of the relevant ICT Manager.

7. The WSTP and its partnership schools reserve the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

8. Property of the WSTP and its partnership schools must be returned to the appropriate location when a trainee leaves the WSTP programme. This includes encryption keys, laptop computers, software, iPads and any other equipment, etc.

Security and Proprietary Information

1. Authorised users are responsible for the security of their passwords and accounts. Log on passwords should be changed when prompted. All users must keep their passwords secure and not share accounts.

2. All PCs, laptops and work stations should be secured, either by locking or logging-off the PC when it is left unattended.

3. Portable computers and laptops are especially vulnerable and so special care should be exercised when using these. Protect laptops by locking them away securely when not in use. Also, do not allow students to use teacher laptops as this may pose a security threat and a breach of the Data Protection Act. Laptops remain the responsibility of the member of staff or trainee to whom they are assigned when not on the school site.

4. If data is taken home or away from WSTP or one of its partnerships schools, it must be on a secure USB Drive. Data removed from WSTP or any of the WSTP partnership school premises in any other format may breach the Data Protection Act and if misplaced or misused, result in prosecution.

5. Postings relating to WSTP or a WSTP partnership school, by trainees. students or employees to social media sites, newsgroups or other blogs are discouraged, but if sent must contain a disclaimer stating that the opinions expressed are strictly those of the sender and not necessarily those of WSTP or the partnership school, (unless the message is sent in the normal course of business.)

6. Users must exercise extreme caution when opening e-mail attachments, web add-ons, popups, especially if received from unknown senders, as these may contain viruses, e-mail bombs or Trojan horse codes. If a school device is infected, please report to the appropriate ICT Manager immediately.

Unacceptable Use

The following activities are, in general, prohibited. Designated employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. system administration staff may have a need to disable the network access of a host if that host is disrupting normal service.) Under no circumstance is a trainee of the WSTP authorised to engage in any activity that is illegal under

local, national or international law while utilising WSTP or any of the WSTP partnership school's ICT resources. The list below attempts to provide a framework for activities which fall into the category of unacceptable use, but is by no means exhaustive.

Prohibited System and Network Activities

The following activities are strictly prohibited and any breaches must be reported to the WSTP Partnership Director:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the use, installation or distribution of "pirated" or other software products that are not appropriately licensed for use by WSTP or the WSTP partnership school.

2. The use of offensive or abusive language in any form of communication or to have any communication that could be considered to be libellous, racist, ethnically or religiously offensive, or that could be construed as defaming a character.

3. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, music, books or other copyrighted sources. The installation of any copyrighted software for which WSTP, their partnership schools, or the end user, does not have an active license, is strictly prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. A member of the Senior Leadership Team should be consulted prior to the export of any such material.

5. The introduction of malicious programmes into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs etc.)

6. Revealing a personal account login id or password to others or allowing use of an account by others. This includes family and other household members when work is being done at home.

7. Using a WSTP or a WSTP partnership school computer to actively engage in procuring or transmitting material that is in violation of sexual harassment or workplace laws.

8. Making fraudulent offers of products, items, or services originating from any WSTP or WSTP partnership school account. Trading on-line in the name of the WSTP or a WSTP partnership school without the express authorisation of the relevant Headteacher.

9. Effecting security breaches or disrupting network communications. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the trainee is not expressly authorised to access, unless within the scope of the user's regular duties. For the purposes of this section, "disruption" includes, (but is not limited to,) network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.

10. Port and / or security scanning is expressly prohibited unless prior notification is made to the ICT Manager and authorised.

11. Executing any form of network monitoring which will intercept data not intended for the employee's host.

12. Circumventing user authentication or security of any host, network or account.

13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

14. Using any program/script/command or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

15. Providing information about, or lists of, WSTP or any WSTP partnership school employees or students to parties outside the school. In particular, releasing the personal details, including phone numbers, fax numbers or personal email addresses of any colleague or pupil over the internet without that persons' agreement.

16. During school hours (8.30am – 3.30 pm) the internet should be used by trainees, students and staff alike for school / educational purposes only.

17. Ensure that children cannot be identified from photographs and ensure that students do not use any personal photographs on a homepage, personal site or learning platform

18. Accessing another users' workstation while they are absent.

19. Trainees, students or members of staff must not access any school server without the express permission of the relevant ICT Manager.

20. Trainees, students and staff are prohibited from using Facebook, Twitter and other social networking sites on any school network. **Prohibited Email and Communications Activities Please see appendix 1.**

1. Emails have the same status as a memo and are the preferred method of communication within WSTP.

2. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

3. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

4. Unauthorized use, or forging, of email header information and / or impersonating another user.

5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

7. Use of unsolicited email originating from within any of the WSTP partnership school's networks and transmitted via other Internet/Intranet/Extranet service providers on behalf

of, or to advertise, any service hosted by the WSTP or WSTP partnership school or connected to, via WSTP or any WSTP partnership school's network.

8. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups, (newsgroup spam.)

Enforcement

Any trainee/employee/student found to have violated this policy may be subject to disciplinary action, up to and including termination of training, employment or suspension. Offences which break the law will be passed onto the police for further investigation.

Appendix 1:

Email Policy

General Information

1. The Email Service

Email service is provided at the host WSTP partnership school to all WSTP trainees for communication purposes both within their school and to email work between school and home. This is a privilege that WSTP partnership schools extend to their trainees. Trainees must observe all the rules governing email service; otherwise, the privilege will be withdrawn. When trainees leave WSTP, the email account will be deleted, unless the trainee remains in employment with the partnership school.

2 Rules:

All trainees using the WSTP email service are required to observe the following rules:

1. Within school, trainees should use only their host school email.

2. For security, no password should be written down or stored on the network. Trainees should not give their password to any other person for any purpose, nor allow another trainee or student to use their email account.

3. Trainees shall not send inappropriate or irrelevant email to other students or a large group of recipients as it will not only waste the recipients' time and their own mailbox quota but also interfere with the normal operation of servers and networks. Typical emails considered as inappropriate are:

a) advertisements;

b) lost and found;

c) announcements to people you do not know;

d) forwarding of jokes; and

e) social email during lessons (email used to chat to friends).

Unsolicited massive emailing is prohibited.

4. Generation or propagation of chain mail is strictly prohibited. Chain mail is equivalent to a chain letter, requesting recipients to duplicate junk mail to others, thus generating a chain of emails.

5. Trainees shall not send email in the name of any other person (fake mail) and shall not use anonymous mail as it is considered as an act of dishonesty. Any fake or anonymous mail may result in disciplinary action.

6. Email should always be written in formal language and observe common courtesy. Text language is not appropriate. Trainees should not use bad language or harass the recipient. Any indecent email is strictly prohibited.

7. Email attachments should not be bigger than 10mb in order to maintain a fast and effective service.

8. The Laws of the UK governing pornographic and indecent material also apply to files stored in electronic forms. Illegal storage and distribution of such material is a criminal offence. All files sent should be copyright free, or the student must be the copyright holder. Trainees should also adhere to the Data Protection Act 1998 and the Data Protection Regulation 2018.

9. A breach of any of these rules may result in suspension or removal of access privilege to the WSTP host school email service.

10. The ICT Manager of the WSTP partnership school hosting each trainee has access to all trainee emails and has the authority to issue warnings to trainees who have breached any of these rules and to deal with the case according to WSTP guidelines.

11. A serious breach of these rules by students will result in disciplinary action.