Stowe School

Pupil Acceptable Use Policy 2017

1) Access to the computer network and services should only be made via your authorised account and password, which should not be made available to any other person.

2) Users are responsible for any activity that takes place under their network account so passwords should be changed whenever a breach of security is suspected.

3) No inappropriate material, including extreme political/religious content should be accessed, stored or transmitted. This rule applies to any computer/device used at School, whether connected to the network or not.

4) The installation of ad hoc software on Stowe computers is forbidden. Users should not run any program that causes files to be installed on Stowe computers or on the network.

5) No computer should be connected to the School network unless it has been configured by a member of the ICT department or connected using the portal of our Network access security system over a web browser.

6) Any computer that is connected to the School's network must have up to date anti-virus software installed on it. Users must contact the ICT Department if they suspect that their anti-virus software is not functioning properly or is not up to date.

7) All School computers configured for connection to the network will have the School's anti-virus software installed on them. Users must contact the ICT Department if they suspect that this software is not functioning properly or is not up to date.

Internet Use

8) Users are responsible for ensuring that all Internet sites and material accessed are of an appropriate nature. Users are expected to avoid any material that is inappropriate and are expected to report any inappropriate sites that get through the School's Internet filtering system to the Head of ICT.

9) When online, users should not do anything that by-passes the School's Internet filtering system, for example by using Internet proxy sites or Virtual Private Networks. Please note URL (Web addresses) are stored - use of inappropriate sites is a disciplinary offence.

Preservation of Bandwidth

10) No file sharing activity, excessive video downloads or multiplayer network games.

11) Any activity that involves the downloading of large files or results in high levels of Internet traffic should be avoided. The size of downloaded files during lesson time should be minimised to avoid issues.

N J Mellor
June 2017

Connection of Personal Devices to the Stowe Network

12) A maximum of 4 devices may be registered for connection to the Stowe Network. If a user is found to have more than 4 devices configured for use on the Stowe Network, all devices registered to that user may be removed from the Stowe Network. It will then be at the discretion of the Network Manager as to whether any of the devices can be reconnected. This directive is essential to protect network resources for the benefit of the connected community.

Email

13) Users are responsible for all email sent and for contacts made that may result in email being received. Secure use, including the use of 'BCC' with non-School email addresses, is discussed in the School e-safety policy available on the School website.

14) It is School policy not to check email randomly but if there are grounds for suspicion of misuse, the account of a user will be frozen and then inspected. It is sensible to assume any email sent on the Stowe network is a public document open to use in all types of judicial hearing.

15) The sending of anonymous or unkind emails is strictly forbidden and may constitute bullying.

Responsible use of the network

16) Work created in non-Microsoft Office software should be converted to a compatible MS format Word) before electronic submission to other Stowe users, unless staff direct otherwise.

17) Office 365- Use of 'sharing' facilities from One Drive in Office 365 should be undertaken with caution as the nature of the document may change over time and become unsuitable for the audience.

18) Pupils should not bring inappropriate films or pictures into the School and any devices or storage containing these materials will be confiscated and appropriate disciplinary action taken. Any large files (eg mp3 or jpg files) not associated with academic work will be deleted from the network. Non academic files should be stored on USB memory sticks, on the hard drive of computers or on CDs and DVDs.

19) All connections to the Stowe School Remote Access site are monitored.

20) Users should store copies of all important work in their "My Documents" on the campus network for safe keeping as this area is backed up daily.

21) The e-safety policy lays out School procedures and policy with regards to safeguarding issues and development of security. Within the behavioural policy the School will detail methods to restrict excessive use of devices as it sees fit.

22) Copyright of materials and intellectual property rights must be respected.

23) Where mobile phones are used to access School email it is vital that the phone is kept secure, with a screen lock, and that the ICT department are notified immediately the phone is lost or mislaid.

24) The amount of data downloaded by pupils is monitored and anyone downloading excessive amounts will have their internet access suspended for a week.

25) Publication of unkind or personal information using SNS or other sites is forbidden and can result in suspension or expulsion. SNS sites must be appropriately secured with appropriate privacy settings before use.

Protection of personal Data

26) Use of tablets, phones and cameras around the School should be curtailed to respect privacy in shared private spaces such as bathrooms, toilets and bedrooms. The School planner lays down further guidance on use of devices. No personal data, including pictures, should be gathered or shared without express permission and it should not in any event be sensitive in nature.

Monitoring of the network

27) The School puts, as top priority, the security of its network and the safety of its users. Action by any user that compromises these aims in any way (e.g., hacking), will be dealt with very seriously, as too will any action that adversely affects the smooth running of the School network.

28) The School reserves the right to examine or delete any files that may be held on its computer system and to monitor and store records of any Internet sites visited, as required by Safeguarding guidelines.

29) The School reserves the right to randomly check the contents of any computer or storage media on the School site. This includes flash drives, CDs, DVDs, MP3 players, I-pods, mobile phones or any other form of storage medium.

30) Any unsuitable material will be deleted, destroyed or kept isolated or when appropriate the matter followed up according to Safeguarding policy.

31) Any large files (e.g. mp3 or jpg files) not associated with academic work will be deleted from the network. Personal files should be stored on USB memory sticks, on the hard drive of personal computers or on CDs or DVDs.

Pupil Section

32) Pupils should not use games that are rated for an age higher than their own age and should only use them during TV usage times and according to guidance with their House.

33) Computers and other electronic devices will be confiscated if it is felt that pupils are not using them appropriately.

34) Whilst at Stowe, Internet access should only be via the School network. Internet access via mobile phones should be via the encrypted Wi-Fi system so that users have the protection of content filters. Pupils should protect their accounts from unauthorised access using strong passwords.

Definitions

1) “Hacking” is defined as any action, malicious or otherwise, that is designed to gain unauthorised access to network, computer or user information or to harm or take control of any computer system.

2) “Inappropriate material” includes any material that is pornographic, offensive, racist, sexist, illegal and any other material deemed by the School to be inappropriate in a School environment.