Acceptable Use Policy for Users of the Stowe Network

Accessing the network

1) You are responsible for all access and activity made via your authorised account and password. This should not be made available to any other person and should be changed often or when compromise is suspected.

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

3) Any computer joining the Stowe network must use the School Network access security system through their web browser.

4) Any personal computer that is connected to the School's network must have up to date anti-virus software installed on it, both updated and switched 'ON'.

5) All School owned 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

6) 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.

7) Web addresses accessed by users are stored - use of inappropriate sites put you your colleagues and the School at risk and is disciplinary offence. 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.

Healthy and effective use of network resources

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

9) During lessons and prep the use of streaming services (YouTube or Netflix) and other media is not allowed unless expressly permitted by a member of staff for a particular use. All devices must be declared to Housemasters/mistresses and must be handed in when required. Housemasters will clarify procedures for this process.

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

Use of Personal Devices on the Stowe Network

11) A maximum of 4 personal 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 and communications

12) Users are responsible for all email received from their School email account. Secure use, including the use of BCC when sending to email addresses outside the School, is discussed in the School Digital Safety policy available on the School website.

13) If there are grounds for suspicion of misuse, the account of a user will be frozen and then inspected. It is therefore sensible to assume any email sent on the Stowe network is a public document open to use in all types of judicial hearing and to adopt a formal tone.

Use of storage and applications (MS Office 365)

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

15) Use of 'sharing' or 'collaboration' 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 original audience. *If a user 'shares' material and then deletes it or leaves the School, they should note it follows the recipient will then lose access to the materials.*

16) Non-academic files should be stored on USB memory sticks, on the hard drive of personal computers or on CDs and DVDs.

17) Pupils should not bring inappropriate films or pictures into the School. Any devices or storage containing these materials will be confiscated and appropriate disciplinary action taken. Any large files (e.g. MP3 or jpg files) not associated with academic work will be deleted from the network.

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

19) Users should store copies of all important work in their "My Documents" or Q drive on the campus network for safe keeping as this area is backed up daily. Materials stored on 'One Drive' will become inaccessible once deleted by the user.

20) The Digital Safety Policy lays out School procedures and policy with regards to safeguarding issues and development of security. The School details methods to restrict access to and excessive use of devices within the 'behavioural policy'.

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

Protection of personal data and privacy - use of non-School devices

22) 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 if the phone is lost or mislaid.

23) Where more than one person can access common publications of any sort e.g. SNS sites, any act which affects other users, including exclusions from groups, unkind declarations or jokes will be treated as bullying and dealt with accordingly.

24) Use of tablets, phones and cameras around the School should be curtailed to respect privacy and is banned in private spaces such as bathrooms, toilets and bedrooms. The Security Policy and Digital Safeguarding instructions on display in Boarding Houses give guidance on safe use of devices. No personal data, including

pictures or videos, should be gathered or shared without express permission of the subject, and it should not in any event be sensitive in nature.

Safety of the network and users - monitoring network security

25) We prioritise the security of the 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.

26) 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.

27) 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, iPods, mobile phones or any other form of storage medium.

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

Pupil only Section

29) 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 within their House.

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

31) Whilst at Stowe, Internet access should only be via the School network. Internet access via personal equipment 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.

Staff Section

32) Staff must follow guidelines issued by the School in the e-safety policy and Staff Handbook regarding the Data Protection Act, MS Office 365 One Drive may be used to access School academic materials with information such as names and academic work in them.

33) Sensitive or confidential materials should be stored in either department (J: drive) or School network My Documents folders (Q: drive) only. Temporary use of encrypted storage such as memory sticks or your School One Drive account may be used where offsite access is required. Take care to remove files that are critical or sensitive to a School storage area on the Q or J drives. NB Staff must specifically exclude access to pages that contain information on Stowenet that they wish to keep private.

34) Use of non-School and 'appropriate' websites for education is governed by the rules in the Digital Safeguarding Policy.

35) Offsite Storage - Stowe's 'Cloud' storage is offered on One Drive, no other third party should be used for personal data. Sensitive and secure data, including medical or psychological assessments, must be accessed on the Q drive using Stowe's secure 'Remote Access System.'

- Please see the Security Policy for further guidance on how to remain secure in external environments such as cafes or family homes.
- Personal devices accessing School services must use secure, password protected Wi-Fi
- Device screens must be set to screen lock after a max of 10 minutes of inactivity
- Access to devices should not be shared with unauthorised users.

36) Social networking- staff should read the Social Networking Policy as detailed in the staff handbook and 'Digital Safeguarding Policy'. Pupils should not be added as friends on staff social sites. Staff should also be aware of the safeguarding guidance issued by the DSL (Designated Safeguarding Lead) concerning prevention of extremist use of SNS sites to influence children.

37) Authorised Access to accounts - Passwords should not be changed in a predictable pattern, not be shared with other accounts and should be changed frequently or if a breach is suspected. Windows and Apollo (MIS) accounts should be logged off and not left unattended. Lost or compromised passwords or other security breaches should be reported immediately. Direct pupils to look away if they are near your keyboard!

38) The School reserves the right to suspend or close network accounts at any time.

Users must note and follow the following Data protection guidelines:

When accessing data:

- Log off or lock your account before leaving it unattended - when using Stowe systems offsite, be especially vigilant
- Keep your password secure and change it frequently to a new one that is not predictable.

Access to personal information:

- Secure (lock) areas or drawers which contain personal information
- Securely dispose of personal or other information when it is no longer needed including deleting it from storage devices/accounts after use and shredding paper documents.

When carrying information:

- Encrypt devices when transporting personal data and log off when you leave the device
- All portable devices will be set to screen lock after 10 minutes of inactivity
- To keep secure or sensitive information backed up on Stowe storage drives.

When giving/sending/storing information/pictures with non Stowe employees/companies:

- Do not send or store any personal information with other companies or persons unless agreed with the Privacy Officer in writing. As a minimum there must be a written agreement with third parties concerning security for the data guaranteeing they will account for data and its subsequent secure protection and deletion. This includes storage providers such as Drop Box.

When publishing information:

Email

- Check forwarded email for sensitive personal information in previous messages before sending it on to someone

- Check private email addresses are in the bcc line
- If unsure, check the full name of internal recipients by pressing the 'To..' button or check names within your Outlook email programme
- To treat all correspondence as if it is on headed company paper for which the School is responsible

Publishing documents Stowenet/365

- Check the audience for new pages on Stowenet or any shared document is the intended one - get help from the IT department if you need it.
- Do not create shared documents from Office 365 'One Drive' accounts and then leave them 'un-owned' so the information is lost.

Please note we take your privacy very seriously and there are notices that clarify who we share your data with and why.

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.

Declaration:

By using the Stowe network, you are confirming you have read and understood the School rules for the use of computers at Stowe School and that you agree to abide by these rules to use the School computer system in a responsible way at all times. You also accept that any breach of these rules might result in disciplinary action.