Acceptable Use Policy

Stoics will accept this agreement on the day they start to use the Stowe 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 by 'Phishing' attack for example.

2) The installation of ad hoc software on Stowe computers is forbidden. Users must not run any program 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 materials accessed are of an appropriate nature. Users must avoid any inappropriate material and are expected to report any sites that breach the School's Internet filtering system to the Head of ICT.

7) Web addresses accessed by users are stored - use of inappropriate sites puts you your colleagues and the school at risk and is a disciplinary offence. When online, users must 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 (You-tube 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

Pupils may only connect phones, laptops with recommended Operating Systems or tablets to the school 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.

E-mail and communications

12) Users are responsible for all e-mail sent from their school e-mail account. Secure use, including the use of BCC when sending to e-mail addresses outside the school, is discussed in the school Digital Safety Policy available on the school web site.

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 mail sent on the Stowe network is a public document open to use in all types of judicial hearing and to adopt a formal tone.

14) Personal e-mail must not be mixed with work related accounts. Please note, school email accounts will only be accessed by IT Staff in accordance with the network Security Policy.

Use of storage and applications (MS Office 365)

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. Use the shared dept drive for materials that are shared and need to be accessed when you have left.*

16) Non-academic files should not be stored on USB memory sticks, on the hard drive of personal computers or any other portable storage.

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 (eg 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) One Drive storage is less secure than local storage on the q drive, and should only be used for files which do not pose a security risk, such as teaching and marking materials.

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'.

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

21) Data from iSams must NOT be downloaded and stored on non-school devices or portable devices that do not have encryption installed on them. Sensitive and medical personal data should not be stored on OneDrive. ANY DEVIATION from this safe practice will result in disciplinary action.

22) Where non-school devices are used (i.e. mobiles phones, personal laptops and tablets) to access school data e.g e-mail or iSAMS it is vital that the device is kept secure, with a screen lock and device encryption. In the event that the phone is lost, mislaid or has a change of ownership, the ICT department must be notified immediately.

23) Where more than one person can access common publications of any sort e.g. Social network 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) Recording media on personal information on tablets, phones and cameras around the school must be with permission 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 gives 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, I-pods, mobile phones or any other form of storage medium.

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

Pupil only Section

29) Pupils should use collaboration software including the schools Teams and other video software in accordance with the integrity and responsibility required when 'in public'. Part of the school policy is to be properly dressed and in surroundings that ensures the privacy of all people in the location of the pupil. Equally pupils should not seek to disrupt or interfere with use of software by staff and pupil for educational purposes by engaging in muting, recording, kicking or any other measures- this will be treated as a serious offence.

30) Pupils should protect their accounts from unauthorised access using strong passwords.

31) Whilst at Stowe, Internet access should only be via the School network. Internet access via personal equipment should be via the school Wi-Fi system so that users have the protection of content filters.

Staff Section

32) Staff must follow guidelines issued by the School in the Digital 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' web sites 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 3rd 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 '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
- Personal Device screens must be set to screen lock after a max of 10 minutes of inactivity
- Access to personal devices which use accounts that access Stowe systems should not be shared with unauthorised users as data or passwords may give unauthorised access to data

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) You must protect your access to school accounts

- Passwords should not be changed in a predictable pattern, never shared with other accounts and must be changed frequently or immediately if a breach is suspected.
- Windows and iSams (MIS) accounts must be logged off, rather than just closing the browser and never left unattended.
- Lost or compromised passwords or other security breaches such as evidence of phishing activity in email should be reported immediately.

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

You must note and follow the following Data protection guidelines:

When accessing data:

- To log off or lock my account before leaving it unattended- when offsite using Stowe systems be especially vigilant.
- To keep my password secure and change it frequently to a new one that is not predictable.

Access to personal information:

- To secure (lock) areas or drawers which contain personal information
- To 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 where they are backed up.

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

- Not to 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 3rd 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:

E-mail

- Check forwarded e-mail for sensitive personal information in previous messages before sending it on to someone
- Check private e-mail 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 e-mail program

- To treat all correspondence as if it is on headed company paper for which the school is responsible

Publishing documents Stowenet/365

- To check the audience for new pages on Stowenet or any shared document is the intended one- get help from the IT dept. if you need it.
- Not to create shared documents from Office 365 'One Drive' accounts and then leave them 'un-owned ' so the information is lost. Department drives should be used for all school documents that are intended to be shared as an essential school resource. Contact IT if you wish to understand how to share school documents with specific groups of staff.
- Tell Pupils if you are recording them and abide by the privacy policy regarding the use of Teams with Pupils.

Please note Staff and Pupil privacy notices 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 unauthorized 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 realise that any breach of these rules might result in disciplinary action.