Acceptable Use Policy

Approved/issue	February 2016	**Locations**	J Drive Appendix to School Handbook Website Headteacher's PA
Review Cycle	2 years		
Next review due	February 2018	**Circulation details**	Governors All staff Parents via website

Definition of Terms

School: Stanborough Secondary School, including the Boarding School International Stanborough School

Headteacher: Headteacher of the School

Pupils, Students: Pupils who attend the School

Staff: Any member of the staff employed by the School in either a teaching or non-teaching role, members of the Governing Body and Volunteers working within the School

Internet: The School-provided Internet system, currently filtered using Smoothwall

Device: any electronic device used by members of the School (PCs, laptop, tablet, phone etc.)

Inappropriate, Unsuitable: anything that falls into the categories of pornographic, racist, extremist, violent or self-harming

Associated Technologies

Anonymous Messages: Messages sent where the sender cannot be identified

Chain Letters: Chain letters are email messages that are sent to convince recipients to make multiple copies and forward them on to their contacts. Chain letters are often sent as a hoax to try and defraud users, or to share important information. They often use emotionally manipulative stories to guilt users to forwarding on the 'chain'

Dynamic Content: the ever changing content on a webpage which is influenced by the user's previous activity.

Executable: an executable file contains a program which can be run by a computer to perform a task which it has been programmed to carry out. These can be harmful because viruses can form part of the programmed coding, of which the user has no control with running.

Microsoft Office 365: Microsoft Apps is a suite of Microsoft applications that brings together essential services such as word processing, spreadsheets, presentations, notes and online storage.

Mobile Device: A portable computing device such as a smartphone or tablet computer.

Personal Hotspots: Personal hotspots are becoming the most popular way in which people tether their devices. Personal (mobile) hotspots emulate a WiFi router so that other devices can connect to it just like they would connect to their WiFi router at home or in school.

Spamming: Refers to the sending of the same message indiscriminately to (a large numbers of Internet users).

Tethering: Tethering refers to accessing the Internet through a mobile phone's connection from any other device. If your mobile device has an Internet connection it can be set up to act as a router for other devices. This means that the Internet can be accessed on a number of devices through one mobile phone's connection.

Virtual Private Network (VPN): A VPN is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

1. Introduction

i) Stanborough School is a caring community founded upon Christian values and, as such, the well-being of each of its members is a prime concern.

ii) Information and Communication Technology (ICT) has transformed the process of teaching and learning in the School. It is a crucial component of every academic subject, and is also taught as a subject in its own right. All Pupils are taught how to research on the internet and to evaluate sources. They are instructed in the importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution.

iii) ICT and the communications revolution provide unrivalled opportunities for enhanced learning, but also pose risks to young people. Pupils are therefore taught how to stay safe in this environment and how to mitigate risk, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

iv) This policy should be read in conjunction with the School Anti-Bullying Policy, the Child Protection Policy and the e-Safety Policy. Significant updates to the policy and/or the agreement may necessitate its redistribution and resigning.

2. Policy statement

i) The purpose of this policy is to protect all users by ensuring that they understand the way in which the School ICT resources are to be used effectively and for their intended purpose. This policy applies to the use of the Stanborough School ICT network, the School internet connection and Devices used on the campus.

ii) Stanborough School encourages pupils to make effective use of the Internet and computer network to enhance their learning and personal development. Such use should always be lawful and appropriate and should not create unnecessary risk or hurt or harm to others. It should not compromise the School's information and computer systems nor have the potential to damage its reputation.

iii) Users are agreeing to all terms and conditions of this policy by logging into, or using, any part of the Stanborough School ICT network infrastructure and also by using Devices on the School campus.

3. Core Principles of Network / Internet Safety

In common with most technologies, Internet use presents risks as well as benefits. Pupils could be placed in inappropriate and even dangerous situations without mediated Internet access. To ensure responsible use and the safety of pupils, the School's policy is built on the following five core principles:

i) **Guided educational use:** Internet use should be planned, task-orientated and educational within a regulated and managed environment.

ii) **Risk assessment:** Both staff and pupils are regularly appraised of the risks associated with Internet use. Where possible, emerging technologies will be examined for educational benefit and a risk on what to do if they come across Inappropriate Material when using the Internet.

iii) **Responsibility:** Internet safety depends on staff, governors, parents and particularly the pupils themselves, taking responsibility for use of the Internet and Associated Technologies. The School will seek to balance education for responsible use with regulation and technical solutions to ensure pupils' safety.

iv) **Regulation:** The use of the Internet, which brings with it the possibility of misuse, will be regulated. Fair rules, written for pupils to read and understand, will be prominently displayed as a constant reminder of the expectations of behaviour regarding Internet use.

v) **Appropriate Strategies:** Effective, monitored strategies will be in place to ensure responsible and safe Internet use. The School will work in partnership with parents and the Internet Service Provider to ensure systems to protect pupils are regularly reviewed and improved.

4. Use of the network

4.1 Logging on and Passwords

Each pupil and the majority of staff are provided, on entry to the School, with a username and password which allows access to the School network. Staff and pupils are responsible for ensuring the security of this password and should under no circumstances pass it on to others. Staff and pupils should not attempt to access the network using any username other than their own. In accordance with school policy, passwords are changed on a regular basis to help ensure that personal information is secure and private.

4.2 Internet Access

All staff and pupil access to the Internet will be monitored and logged.

Unintentional Exposure of Pupils to Undesirable Materials

It is the School's policy that all reasonable steps should be taken to prevent the exposure of pupils to undesirable materials on the Internet. It is recognised that this can happen, not only through deliberate searching for such materials, but also unintentionally when a legitimate Internet search yields unexpected results. Furthermore, due to the dynamic content of some websites, not all content can be checked before students access them, for example, the video links which are suggested on YouTube when videos are accessed.

To prevent such occurrences the School's Internet is "filtered" with the intention of:

- Implementing a frequently updated list of Unsuitable sites
- Filtering sites by language content
- Blocking undesirable network traffic such as illegal downloading

In the unlikely event that pupils are unintentionally exposed to Unsuitable materials they should switch off their monitor and notify a teacher immediately. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported immediately to IT Support, who will then take further action. The School cannot accept liability for the material accessed, or any consequences of Internet access, but will attempt to remedy any issues which arise.

4.3 Social Media

i) Pupils will be held personally responsible for all material they have placed on a website including social networking sites such as Facebook, Twitter, Instagram, etc. and for all material that appears on a website for which they are the account holder.

ii) Pupils should not access the Internet via any personal or portable device to obtain any material which may be deemed inappropriate e.g. pornographic, violent, racist and extremist material, and this also includes the use of chat rooms.

iii) Because the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990, staff and pupils will be made aware that such inappropriate use will be treated seriously by the School.

4.4 Staff Access

Staff will be encouraged to use this resource to support and enrich their own teaching, job execution and professional development. Staff will observe all restrictions and policies with regards to appropriate use of the Internet. Any complaint about staff misuse must be referred to the Headteacher.

4.5 Boarding

i) Boarding pupils Year 9 and above are permitted to access specific social networking sites, such as 'Facebook' and to use 'Skype' to communicate with family and friends, at specified times. The Boarding Preceptor in conjunction with IT Support will decide which websites are acceptable and at what times. The usage of such websites is conditional on attending an induction on the safe use of the Internet, which will be provided in the first half term of the school year.

ii) Boarding pupils are permitted to use mobile phones at specified times within the boarding community. They are not permitted to be used during prep or after bedtime, unless permission from their Preceptor/Preceptress has been granted.

iii) Boarding pupils Year 7, 8 are not permitted to access social networking sites while in the care of the School.

4.6 Wireless network and Devices

Boarding Pupils may connect Devices to the Boarding School's wireless network via the Pupil WiFi (boarding). When prompted they must login with their School network credentials. In the Boarding School all connections to the Internet must be made via the Boarding School network and thus via its web filter. Pupils should not use personal connections to the Internet (for example 3G or 4G). Any pupil who bypasses the School web filter or breaches the rules outlined in this Policy by using a personal connection to the Internet, will be subject to the same disciplinary procedures as when misusing the School's own ICT facilities. The use of mobile internet may also incur charges from the network provider.

4.7 Tethering & Personal Hotspots

Pupils should not tether their Devices or create personal hotspots within the School campus in order to bypass the School's filtering system. The School's ICT network scans for such activity and records the details of these devices. Sanctions may be imposed for pupils who are identified as breaching this rule will be disciplined in line with the e-Safety policy.

4.8 Use of Printers

The following rules and guidelines are to be observed:

i) Printing facilities, from the ICT network, are provided for academic work or activities related to organised extra-curricular activities, not for personal use.

ii) Pupils must take care to ensure that they do not print excessively or unnecessarily and are encouraged to discuss with their teachers other means of submitting work, e.g. by sharing a document on OneDrive or shared network drives.

iii) The School will determine printing limits and also control the location and times that printing may be done.

4.9 Installing Hardware and Software

The installation of hardware and software on the network is the sole responsibility of IT Support. Pupils and staff are forbidden to install software into their user area or anywhere else and therefore executable files should not be present. Staff should consult with the IT Manager if they wish to have software installed or if they need hardware installing or relocating. Failure to follow the above requirements regarding software installation may result in contravention of Copyright Designs and Patents Act 1988. Pupils who are identified as breaching this rule will be disciplined in line with this policy.

4.10 Sharing Material (E-mail and Microsoft Apps)

i) Each pupil has their own e-mail address on the School's networked system and their own Office 365 account. Only these approved e-mail and Microsoft App accounts may be used by pupils.

ii) Web-based e-mail is not available to pupils in school and all access via the School's e-mail system will be logged. The reception of inappropriate e-mails from outside school (e.g. SPAM) will be controlled and filtered by the School. Certain types of attachment, e.g. executables and those that might contain viruses, will be blocked.

iii) Pupils should not send any e-mail that might be considered as inappropriate. The sending of hurtful and inconsiderate e-mails to fellow pupils may be classed as cyberbullying, and will be dealt with accordingly. Cyberbullying is a particularly pernicious form of bullying, because it can be pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. The School's Anti-bullying Policy sets out our preventative measures and the procedures that will be followed where we discover cases of bullying. Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to report the matter.

iv) The personal safety of Pupils is strongly encouraged within the School and as a result:

- Pupils should not share personal information, e.g. mobile numbers, home address or e- mail address in order to sign-up/subscribe to any website;
- Pupils should not arrange to meet anyone they do not know through e-mail communication, nor should they share contact details of themselves or others, e.g. address or telephone numbers;
- If pupils receive an offensive e-mail they should report this to a member of staff.

The following rules and guidelines are to be observed:

i) The School e-mail system is the only e-mail system to be used in connection with School activities. The School e-mail address should therefore be used as the contact point for any electronic communication by pupils related to academic work or educational activities with external organisations e.g. UCAS or university admissions departments.

ii) Electronic messaging between pupils and teachers must use the school e-mail system and not third-party e-mail providers (e.g. hotmail, Yahoo, Gmail, etc.) or messaging systems from social networks such as Facebook. Similarly, sharing material on Office 365 should be done using the pupil's school account and not a personal account.

iii) Pupils should only add their School e-mail address with the parent or guardian's permission, although the School does encourage this.

iv) The system can be used for both School and personal use in accordance with School policies.

v) The School has its own virus scanning software which regularly scans all files on the network and attachments sent through email. Users must take all reasonable steps to ensure that they do not open any emails and /or attachments from unknown sources.

vi) Users should exercise caution when opening any e-mails from companies, organisations or persons not known to them. If they are unsure then they should ask IT Support for help, via their Form Tutors or Senior Teacher.

vii) Spamming is forbidden.

viii) Posting Anonymous Messages and forwarding Chain Letters is forbidden. Chain letters commonly contain viruses, or hoax threats.

ix) There is a finite limit on the number, individual size and total size of e-mails that can be kept in an individual's account. Therefore staff and pupils are encouraged to share files and attachments through OneDrive or shared network drive instead of e-mail.

5. Unsupervised and Recreational Use of ICT facilities

i) Pupils are permitted access to ICT facilities outside of normal contact time at the School's discretion. This use is monitored by IT Support and anyone found to be breaching the e-Safety policy may have their access revoked. Recreational use is permitted during break and lunchtimes and after school. However, users must still follow the rules of use for ICT facilities and should be aware that several non-academic sites, e.g. game-playing websites, may be blocked by the School's web filter. Academic work will always be given priority and a user may be asked to vacate a facility that is being used for recreational purposes if it is needed by another user for academic work.

ii) Outside of directly supervised lessons and private study sessions, pupils may access a school computer without direct supervision. They are reminded, however, that the School supervises all Internet activity and that they must adhere to the rules set out in this policy at all times. Access at break time (Monday – Friday 11:10-11.30am) and lunchtimes (Monday – Thursday 1.30-2.20pm) in the Library will be supervised by staff on duty. Pupils are not allowed to access the network or the Internet using any of the computers in classrooms, unless they are supervised by a member of staff.

6. Unauthorised use of the ICT Facilities

Pupils are NOT permitted under any circumstances to:

i) Utilise a 3rd-party e-mail service (using Hotmail etc.) via the School network.

ii) Utilise a VPN (Virtual Private Network) to access any system either within or outside of Stanborough School's IT Network.

iii) Access social networking sites via the School network during school hours.

iv) Use the ICT facilities for commercial or financial gain.

v) Interfere with the ICT facilities in any way.

vi) Use or attempt to access someone else's account.

vii) Pupils must never intentionally seek offensive material on the Internet. They may not use the ICT facilities at any time to access, download, send, receive, view or display any of the following:

- Any illegal material.
- Any message that could constitute bullying, harassment or any negative comment about other persons or organisations.
- Remarks relating to a person's sexual orientation, radicalisation, gender assignment, religion, disability, age or ethnicity.
- Online gambling sites.
- Remarks which may adversely affect the reputation of any organisation or person, whether or not pupils know or believe them to be true.
- Any sexually explicit content.

viii) All forms of piracy, including the infringement of software licences or other copyright provisions, are illegal. This includes copying, downloading or distributing material from the Internet or e-mail such as computer software, music, text, and video clips. Pupils must not do

so if it is not clear that they have the permission of the copyright owner or if the permission cannot be obtained.

ix) Within lessons, the use of unauthorised games or messaging services is forbidden.

7. Discipline Guidance

Any transgression will be reported and recorded. Any incident will be treated as a disciplinary matter and a pupil's parents/guardians may be informed.

If the breaking of the rules of use is found to be significant, repeated, flagrant or habitual, the matter will be treated as a serious disciplinary issue. A pupil's parents/guardians will be informed and the School's Governing Body will be advised.

i) Violations of the rules outlined in this Acceptable Use Policy will result in a temporary ban on Internet and/or e-mail use.

ii) Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.

iii) When applicable, the Police or Social Services may have to be involved.

8. School Computer Network Guidelines Acceptance & Permission Form

These rules will keep everyone safe and help us to be fair to others.

- I am aware that all of my Internet activity within school is logged, whether it is accessed on a School computer or personal mobile device.
- I will use the School's computers for only school work, homework and as directed.
- I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace.
- I will edit or delete only my own files and not view, or change, other people's files without their permission.
- I will keep my logins, IDs and passwords secret.
- I will always make sure to logout off the computer before leaving it unattended and will remove all media from their drives
- I will not eat, drink, groom and use aerosol sprays near a computer
- I will not switch off or restart a computer during the school day unless it has completely locked up (excluding a lock being forced by LanSchool)
- I will use the Internet responsibly and will not visit sites I know to be banned by the School. I am also aware that during lessons I should visit only the websites that are appropriate for my studies.
- I will e-mail only people I know, or those approved by my teachers.
- The messages I send, or the information I upload, will always be polite and sensible.
- I will not open attachments, or download a file, unless I have permission or I know or trust the person that has sent them.
- I will not give my address, phone number, send photographs or video, or give personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by e-mail or in a chat room, unless I have a trusted adult with me.
- If I see anything I am unhappy with or receive a message I do not like, I will not respond to it but will save it and talk to a teacher/trusted adult.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
- I will not set up a personal hotspot on my mobile device, nor tether my Internet connection to other devices.
- I will not bypass the School's Internet filtering system by using 3G or 4G on my mobile device.

I have read these guidelines and agree that it is my responsibility to follow them in School.

Pupil's Full Name *(capital letters):* _____ Year group: _____

Pupil Signature: _____ Parent/Guardian Signature: _____

Date: _____ Date: _____

Sanctions

1. Violations of the above rules will result in a temporary ban on Internet and/or e-mail use.
2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
3. In extreme circumstances the Social Services, Channel officer or Police may be involved.