INTRODUCTION

This policy should be read in conjunction with the Child Protection Policy.

This 'Pupil Acceptable Use' policy is intended to ensure that:

- Pupils will be responsible users of IT and stay safe whilst using the internet and other Information and Communications Technologies (ICT) at Charterhouse.
- School Information and Communications Technologies systems (ICT) and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- The School will ensure that pupils will have good access to Information and Communications Technologies (ICT) to enhance their learning and will, in return, expect the Pupils to agree to be responsible users.

SECURITY

Access to School's systems

Access to School's systems is provided and it is your responsibility to keep your username and password safe and ensure that others do not gain access to it. Should you suspect that someone has access to your account then you should report it immediately to your Housemaster and the IT department.

Pupils must not gain or attempt to gain unauthorised access to any computer system for any purpose. Such hacking or attempted hacking is a criminal offence under the Computer Misuse Act (1990).

School Information and Communication Technology systems (ICT) are primarily intended for educational use. Time restrictions, for personal use of the Internet, apply throughout the day and all content is filtered, details of which can be found on Greyhound.

Anti-virus

In order to protect against a virus threat, anti-virus software is installed and updated regularly on all School PCs. It is the pupil's responsibility to ensure any personal devices have up-to-date antivirus software installed. Pupils must ensure that this antivirus software is kept up to date. Pupils should not open any attachments to emails unless they know and trust the person/organisation that has sent it, due to the risk of it containing viruses or other harmful programs.

INTERNET AND INFORMATION AND TECHNOLOGY SYSTEMS USAGE

Network access and downloading content

All pupil internet access must be via the School's wired or wireless network.

Pupils must not use the School's network or any other service or device to make, download, view, store, possess, show, print or share illegal material. This includes images of anybody under 18 which might be deemed to be sexual (e.g. 'nudes'). Even for a child, making, viewing or sharing a sexual image of someone under 18 is technically a criminal offence, and the School will address it as such.

Pupils should be aware that, as the internet is a global network, some activities/material which may be legal in the UK, may be illegal elsewhere in the world and vice versa. If you are in any doubt as to the legality of anything, don't do it.

Pupils are advised that with any downloading of material (such as files, music, videos etc.) via the Internet, to exercise judgement and think of how it may affect others, as bandwidth can become slow and unresponsive under heavy usage. Unsafe sites and certain types of files maybe blocked. Sharing of files and downloading of files over peer to peer network connections is forbidden at all times. Only School related media files may be stored on the School network.

Pupils should shut down their computer/laptop when not in use, and computers/laptops should NOT be left unattended whilst downloading.

Any comments or pictures added to social networking sites should adhere to the School Behaviour rules that require pupils to be responsible, thoughtful, and considerate. For example, pupils must not record or film arguments, fights or other altercations amongst peers and then post them on social media for amusement or any other reason.

Accessing the Internet via a third party 'proxy' website (VPN) is not permitted.

Cyber-bullying

Cyberbullying is defined as the use of modern electronic technology to bully other people. It may involve email, mobile phone and text messages, instant messaging, personal websites and/or chat rooms. Any suspected cyberbullying (whether during School time or otherwise) will immediately be reported to the Deputy Headmaster (Pastoral), and will be addressed under the School's Anti-Bullying and Cyberbullying policies.

Charterhouse email

Pupils are allocated an email account for internal and external email. All pupils are by default configured to access their Charterhouse email via the Internet. To do so, from an Internet browser, you should go to the following link – http://portal.office.com/

Printing

Printing facilities are provided and pupils are encouraged to print only when absolutely necessary in order to minimise the impact on the environment. Colour printing should only be used if the pupil's work requires it. Duplex printing should be used wherever possible.

Mobile devices/video recording

Please refer to the School's Mobile Computer Device Policy, a copy of which can be found on Greyhound.

Monitoring

In accepting the School's IT Pupil Acceptable Use policy, you consent to the School's monitoring and recording any use that you make of the School's electronic communication systems, including mobile phones, for the purpose of ensuring that the School Rules are being complied with and for legitimate business purpose.

Health issues and Wi-Fi

The latest information provided by the UK Government and the World Health Organisation reports that there is no consistent evidence that exposure to RF signals from Wi-Fi and WLANs adversely affect health. Consequently, Charterhouse will continue to offer Wi-Fi in both academic and pastoral areas, and will continue to monitor the advice from these organisations.

Key points from the GOV.UK (Public Health England) guidelines on exposure to radio signals from wireless networks (Wi-Fi). First published 1 November 2013.

- *There is no consistent evidence to date that exposure to RF signals from Wi-Fi and WLANs adversely affect the health of the general population.*
- *The signals from Wi-Fi are very low power, typically 0.1 watt (100 milliwatts), in both the computer and the mast (or router) and resulting exposures should be well within internationally-accepted guidelines.*
- *The frequencies used are broadly the same as those from other RF applications.*
- *Based on current knowledge, RF exposures from Wi-Fi are likely to be lower than those from mobile phones.*
- *On the basis of current scientific information, exposures from Wi-Fi equipment satisfy international guidelines. There is no consistent evidence of health effects from RF exposures below guideline levels and no reason why schools and others should not use Wi-Fi equipment.*

Please sign to confirm having read and understood this policy. If there is anything you do not understand, or if you require any further information or advice on any IT related topic, please contact IT Support on ext. 646 or email itsupport@charterhouse.org.uk.

Print your name ……..

Pupil's signature …… Date ……