St John's School
LEATHERHEAD

Internet Acceptable Use Policy

Date of Issue:	9 March 2012
Date of Review:	September 2017
Responsible Person:	IT Support Manager

Scope

This Acceptable Use Policy (AUP) applies to all St John's School staff (including temporary staff), visitors, contractors, pupils and to those using the school's IT resources. For the purposes of this document the 'internet' is defined as; web services, chat rooms, bulletin boards, newsgroups, peer to peer file sharing, instant messaging software and social networking sites.

General Principles

- Use of the Internet by school staff, pupils and contractors is permitted and encouraged where such use supports the goals and objectives of the school.
- Use of Internet is monitored for security and/network management reasons. Users may also be subject to limitations on their use of such resources.
- A web filtering system is employed within school to enforce some restrictions including user authentication.
- The distribution of any information through the School's network is subject to the scrutiny of the School. The School reserves the right to determine the suitability of this information.
- The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately. For example the Police can have a right of access to recorded data in pursuit of a crime.
- The School has the right to refuse access to the network for any device, if the school is not satisfied that appropriate anti-virus or security software has been installed.

Unacceptable Use or behaviour:

It is unacceptable to;

- Visit Internet sites that contain obscene, hateful or other objectionable materials (unless this has been approved by a member of the Senior Management Team)
- Make or post indecent remarks, proposals or materials on the Internet including racist or sexist jokes and defamatory comments.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the School, or the School itself unless this download is covered or permitted under a commercial agreement or other such licence.
- Download any software or electronic files without implementing virus protection measures that have been approved by the School.
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network
- Monitor Network Traffic Content or scan devices connected to the network.

Users should:

- If you become aware that there has been unauthorised access to your computer, you must raise it immediately with the IT Support Department because of the implications for the security of School, and personal data.
- Record any instances where you have accessed inappropriate sites by accident. For example this may be through mistyping an address or spam email link.
- Log out of the computer when you have finished

Monitoring

The School accepts that the use of the internet is an extremely valuable business, research and learning tool. However misuse of such a facility can have a detrimental effect on other users and potentially the School's public profile. As a result, the School monitors;

- The volume of internet and network traffic and the internet sites visited.
- The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

We are obliged to monitor to fulfil our responsibilities with regard to UK law.

Action as deemed appropriate by the IT Support Manager and, if required, other representatives such as the HR Manager or Senior Management Team may be taken.