IT Acceptable Use Policy

Date of Issue:	November 2017
Date of Review:	September 2018
Responsible Person:	IT Network Manager
References:	E-Safety Policy
	Safeguarding and Child Protection Policy and Procedures
	School Rules
	Code of Conduct

Scope

This Acceptable Use Policy (AUP) applies to all members of the St John's School staff including contractors. Pupils, volunteers and visitors who use the School's IT systems will also be asked to sign an acceptable use agreement.

For the purposes of this policy "IT" includes (but is not limited to) the School's computers and telecommunications systems, networks, hardware, software, servers, file storage systems, email, internet and web services, applications, file sharing, instant messaging software and social networking sites.

General Principles

Use of IT is permitted and encouraged where such use supports the goals and objectives of the school. Whenever you use the School's IT systems (including by connecting your own device to the network) you should be aware of and follow these principles:

- Your use of IT is monitored for security and/network management reasons. You may also be subject to limitations on your use of such resources.
- A web filtering system (Smoothwall) is employed within School to enforce some restrictions including user authentication. To connect your own device you will be required to have a Smoothwall certificate installed onto it. Do not attempt to circumvent the content filters or other security measures installed on the School's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- 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 IT 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.
- You should only access School IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to install software on, or otherwise alter, School IT systems.
- Remember that the School monitors use of the School's IT systems, and that the School can view content accessed or sent via its systems.

Online behaviour

As a member of the School community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others.

- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the School community (for example, content that is obscene, or promotes violence, discrimination, or extremism). Accessing pornographic material is considered an act of gross misconduct (see School Rules) which will result in your dismissal without notice.
- Some misuse of IT will lead to disciplinary action, but all members of the School community should note that the age of criminal responsibility in England and Wales is 10 years, and that it is a crime for anyone from that age to take, possess, make (by downloading), or distribute any image or pseudo image of a child or young person under 18 years considered indecent, or sexual.
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- As per the Code of Conduct, Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Users of School IT systems should:

- Record any instances where you have accessed inappropriate sites by accident. For example this may be through mistyping an address or spam email link.
- 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.
- Lock computers and devices whenever they are unattended and log out when you have finished.

Monitoring

The School is obliged to monitor IT and internet use to fulfil its safeguarding duty and responsibilities under UK law. Inappropriate use of IT can expose the School and the user to significant liability. For further detail please see the Monitoring Policy.

Compliance with related School policies

Acceptable use of IT, internet and social networking is covered in other School policies including the School's e-Safety Policy, Safeguarding and Protecting Children Policy and Procedures, School Rules and Code of Conduct. You will ensure that you comply with these Policies.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter in accordance with the Disciplinary and Dismissal Procedure.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Deputy Head and/or refer to the Whistleblowing Policy and Procedure. Reports will be treated in confidence.

Acceptance of this policy

Please confirm that you understand and accept this policy by signing below and returning the signed copy to Christine Goble, HR Manager.

If, after reading and agreeing to this, you have any questions or concerns about your own or another's use of the internet to view pornography, or behaviour in chatrooms, you can get confidential advice at the helpline *Stop it Now UK*, online (www.stopitnow.org.uk) or by phone at 0808 1000 900. You should also report any content which concerns you to the Internet Watch Foundation, www.iwf.org.uk.

I understand and accept this acceptable use policy:

Name: ……

Signature: …… Date: ……