ICT ACCEPTABLE USE POLICY

E – Safety

E-Safety is an important part of keeping children safe at St George's School. We have extensive security measures in place in school, which are monitored both internally and externally, to help safeguard students from potential dangers or unsuitable material. Any e-safety incidents are managed in accordance with our E-Safety Policy. E-Safety is taught to all students in specific lessons, explaining and demonstrating how to stay safe and behave appropriately online.

Ground rules

Discuss as a family how the internet should be used in your house. Consider what should be kept private online and decide rules for making and meeting online friends with your parents. Do not arrange to meet anyone face to face that you have spoken to online.

Online safety

Speak to parents/guardians about Installing antivirus software, secure your internet connection and parental control functions for computers, mobile phones and games consoles to block unsuitable content or contact.

Location

As a family, look to locate your computer in a supervised family area. Involve parents/guardians in the supervision and use of webcams and applications which allow voice or video chat.

Dialogue

- Talk to your parents/guardians and teach them how to use the internet, share what you know and have learnt about safe internet use at school with them. Learning together can often open opportunities to discuss safe behaviour.
- Always speak to parents/guardians about any nasty or inappropriate messages or content you receive. Look to block or delete any contacts who involve themselves in this activity. Do not retaliate or reply. Screen shots should be kept as evidence, if needed by appropriate agencies to pursue and take necessary steps of action.
- Tell an adult you trust if you see something online that makes you feel scared, worried or uncomfortable.

Helpful websites to search and to help inform you on these areas are:

Educate Against the Hate, CEOPS, ThinkUknow. Internet Matters, NSPCC Share Aware, CBBC Stay Safe, Kidsmart, Childnet International.

IT Equipment (including cabling)

- Treat all equipment with care and respect so as to cause it no damage.
- Do not use any equipment that you believe to be damaged or unsafe.
- Report immediately any damage to the equipment that you become aware of.
- Do not dismantle, remove or relocate any part of the equipment.
- If you are aware of anyone damaging, stealing or misusing equipment you must report it to a teacher or member of senior staff immediately.
- Do not eat or drink whilst using IT equipment.
- Do not connect any equipment or device to the network without the prior approval of the IT Technician.

Software

- Do not install or attempt to install, programs of any type on a machine, or store programs on the computers without permission.
- Do not deliberately damage, disable or otherwise harm the operation of software on computers.
- Do not deliberately create, distribute or install agents designed to, or are likely to hamper, disable, disrupt or damage any part of the system.
- The distribution or storage by any means of pirated software is prohibited.

Mobile devices

- This applies to all mobile devices e.g. Laptop / notebook / netbook / tablet / memory sticks / USB storage Media / PDAs / phone, etc.
- The use of private equipment during lessons is forbidden unless authorised by a teacher.
- Any mobile device brought onto school premises should be virus free and checked on a regular basis by the owner.
- Data must not be downloaded and copied from the network or attached machines unless you have lawful and appropriate authority to do so.
- All mobile devices should be password protected and all data encrypted.
- The school reserves the right to refuse connection to the school network.
- Any such equipment is brought into school at the user's own risk.

Passwords and Security

- Do not disclose your password to others, or use passwords intended for the use of others.
- Passwords used must adhere to current password policy and practice.
- Do not disguise, attempt to disguise or mask your identity.
- Do not attempt to bypass security in place on the computer systems.
- Do not attempt to access any username or email address, which is not yours.
- Do not access, copy, remove or otherwise alter other people's work.
- Do not attempt to alter the settings of computers unless authorised to do so.
- All network activity and online communications are monitored.

Internet rules

- The school monitors internet usage.
- Only access the internet for study purposes or school authorised activity.
- Do not use the internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- You must report any accidental accessing of unsuitable sites to a teacher.
- Students are expected to respect copyright laws at all times.
- Do not engage in game activities over the internet or download such games.
- Do not engage in chat activities over the internet other than through approved educational forums authorised by the school.
- Do not give personal information such as your address or telephone number to those whom you contact through electronic mail or websites.
- No communications device (this includes mobile phones), whether school provided or personally owned, may be used for the bullying or harassment of others in any form.

E-mail

- Pupils must only use their email account and must not allow anyone to use theirs.
- Appropriate language must be used at all times.

Social networking websites and online forums

- The use of Facebook, Bebo, Twitter, My Space, Snapchat, Instagram, Musical.ly, Tumblr, Whatsapp, Youtube and other similar social networking or chat room sites are not allowed on the school premises.