Staff ICT Acceptable Use Policy

School Computers and Mobile Devices

For the purpose of this document, any portable computing device such as a smartphone, laptop or tablet will be referred to as a mobile device.

Users **are not** permitted to undertake any of the following actions:

1. Log on to the network with another user's account.
2. Plug a mobile device directly into a physical network socket or switch.
3. Use computers or mobile devices to send offensive or harassing material to others.
4. Tamper with computer hardware or software.
5. Attempt to gain access to the local drive of any school computer.
6. Attempt to share any drives or folders from a mobile device on the school network.
7. Attempt to gain access to unauthorised areas of the network.
8. Use VPN clients or any other software attempting to circumvent the school's web filter.
9. Access inappropriate web sites.
10. Attempt to spread viruses via the network.
11. Attempt to create any type of script or executable while connected to the school network.
12. Use school computers or mobile devices for any form of illegal activity, including software and music piracy.
13. Use any software which is not installed on a school computer. This includes software stored on USB sticks/external hard drives or software downloaded from the internet which have the ability to run directly from a user's profile.

Data Protection

1. Staff must not store school related files in the cloud unless it's a school-managed cloud environment.
2. Staff must not store school related files on external storage devices.
3. Personal mobile devices that are connected to school services including WiFi and/or Email must not be using a shared user profile. If the device is shared amongst family members, separate user profiles must exist.
4. It's advised that a password should not be used for multiple purposes. E.g. your school password should not be the same as the password you use for Facebook. If one account is compromised, it opens up access to all of your online accounts. Your school password allows access to potentially confidential information within our management information system so should be unique.
5. If a device is lost or stolen and it's been used to access your school email or files, please inform the Helpdesk right away to obtain advice on wiping the data.

Breach of the acceptable use policy may result in disciplinary action being taken.

Reviewed SJPF/RXM September 2018

ICT Helpdesk – helpdesk@ipswich.school