City of
London
School

City of London School Acceptable Use of Computers Policy (Pupils)

Introduction

Any large computer network is a highly complex system requiring a considerable amount of maintenance. The points below are designed to ensure that the network is always available and working at the appropriate times. All users of the network (whether using school computers, personal laptops or any other device that can connect to the school network by whatever means) are expected to use their common sense, the more general School rules and regulations and the law of the land. This policy also applies to any access to the internet or the school system using 3G, 4G, wireless or any other technologies whilst at school or under school control.

System Security

Boys are responsible for their individual account and must never allow anyone else to use it, even when they are present. Passwords should never be divulged to another person. Passwords should be changed at least once per term. Passwords should be at least 7 characters in length and contain at least one capital letter and one numerical character.

Unauthorized Activities

Boys should not attempt to go beyond their authorized access. This includes attempting to log in through another person's account, sending e-mails while masquerading as another person, or accessing another person's files in their directory. No-one must make deliberate attempts to disrupt the computer system or destroy data. Boys should also not attempt to deceive other external secure websites through the school network.

Social Networking Sites

Boys should not post personal information to social networking sites such as YouTube, Facebook, Instagram and Twitter if such information would allow others to find out details of where a person lives. Such sites, used sensibly, can provide genuine opportunities for keeping up with friends, sharing resources and learning, but everyone must be aware that other users may not necessarily be who they say they are. No-one must use such sites to impersonate others, nor to participate in any form of “cyber-bullying”. Nothing must be posted on such sites which identifies the School with unacceptable opinions or activities, or which would bring the School into disrepute. Social Networking sites should not be accessed during lesson time without the express permission of the teacher for the purpose of teaching and learning.

E-Mail

No indecent, obscene, offensive, or threatening language can be used, nor should anyone engage in personal, prejudicial, or discriminatory attacks. At all times, privacy should be respected concerning any messages sent and no messages should be re-sent or forwarded to others without permission. Boys must not use their personal email addresses for communicating with members of staff. They may only use their City of London School email for communicating with members of staff.

Internet Access

Computers at School or other devices which can link to the school network or the internet whilst at school (or whilst under school control) must not be used to access material that is profane or obscene, that advocates illegal acts, violence, or discrimination towards other people. If inappropriate information is mistakenly accessed, the tutor, Head of Year or another teacher should be informed immediately. This action will protect boys against the accusation that the material was intentionally accessed. Boys must not plagiarise works found on the internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were one's own. Copyright must be respected. The internet must not be used to download illegal software or, for example, pirated music, images or films.

Devices

The rules that apply to School computers also apply to boys' own devices when brought to School. Boys should ensure that any unsuitable material (as defined in the previous paragraph) is deleted before bringing it to School. Boys should not be allowed access to each other's devices. Technologies such as 3G, 4G or wireless should not be used to gain unfiltered web access. If there is a suspicion that a boy has broken these rules, a member of the Senior Management Team or system administrator may seek access to the boy's device, prior to an investigation taking place.

Respecting Resource Limits

Large files should not be downloaded or saved unless absolutely necessary as this can restrict others' use of the network. This also applies to the streaming of films or television via the school network. (Boys should respect the age classification of films they are watching). School emails should be checked frequently and any unwanted messages deleted promptly.

Privacy

Boys should expect only limited privacy in the contents of their personal files on the school system or on their laptop if used to connect to the system. The system administrators, the Head of Year, and parents or guardians have the right at any time to require access to a boy's School directory or laptop. As a general rule, boys should not store anything which they would feel uncomfortable justifying in front of any member of staff or their parents.

Sanctions

When using the school's system, boys may think that it is easy to break the rules above without the risk of detection. However, whenever the network is used, an electronic trace is left that can subsequently be followed. Depending on the severity of the offence, one or more of the following sanctions may be applied if a boy is found to have broken any of the above rules:

· A formal warning

· Suspension of internet access

· Suspension of computer system account

· Laptop confiscation

· Debarment from use of the school computer rooms

· Formal school detentions

· Temporary or permanent suspension from the School

Policy reviews: January 2016 CBS