



Burscough Priory Science College

Acceptable use of Curriculum Network, Associated Systems & Cyber Safety Agreement

The school network and associated systems are owned and managed by Burscough Priory Science College and made available for use at the school's discretion. No user is entitled to use of the systems and gross misuse will result in denial of access. The statement has been drawn up to protect all parties. The school reserves the right to examine and delete any files held on the system, to monitor any Internet sites visited and email sent between students.

All of this is in accordance with Data Protection, Laws of Copyright and the Education and Inspections Act 2006 (EIA 2006).



Network, Internet and E-Mail

- Use of internet & email by staff & students is permitted and encouraged where such use is suitable for education purposes and supports the goals and objectives of the school. Internet & Email is to be used in a manner that is consistent with the school's standards of conduct.
- School email accounts are to be used for education purposes only. However, limited personal use is acceptable. User account access should only be made via the authorised account to the assigned student.
- The school reserves the right to directly access students' accounts in the pursuit of an authorised legal or disciplinary investigation. The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately (the Police have right of access to recorded data in pursuit of a crime).
- Use of internet and email may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources.
- The distribution of any information on the school's network is subject to the scrutiny of the school, who reserve the right to determine the suitability of this information.
- The use of E-Mail attachments within messages is strictly limited to professional and educational purposes only. Users found to be sending unfit E-Mail attachments may be subject to having their privilege to use the system revoked. Abuse towards other users via email and forwarding chain letters is forbidden.
- Use of the network to access and publish inappropriate materials such as pornographic, racist and of an offensive nature is strictly forbidden.
- Copyright of materials must be respected and acts of plagiarism are strictly prohibited.
- Network resources provided to students must be respected and any problems must be reported to the ICT Support Department. Students must not share account passwords or allow other students usage of their account, as account responsibility lies with the student whom the account has been assigned to.
- Pupils are not permitted to use personal laptops within school or on the school network, unless as part of a fully documented Special Educational Need, or with prior permission from the ICT Support Department.

- Use of removable storage is permitted and is the sole responsibility of the student. The school will not take responsibility for data loss or loss/damage to removable storage devices.
- Use of remote desktop off-site is provided to all staff and students, but misuse of this service may result in suspension of access or an indefinite block on the account being used off-site.



Cyber Safety and Anti-Bullying

The school has a duty to protect all its members and provide a safe healthy environment to work in.

You are advised never to reveal any personal information about yourself or anyone else (for example: email address, social media accounts, mobile number, telephone number or home address).

It is against the law for any student to access social networking sites before the age of 13, such as Facebook; underage access can be used as a potential vehicle of exploitation by adults.

- The use of Information Communication Technology (ICT), particularly mobile phones and the internet to deliberately upset someone else is strictly prohibited.
- The head teacher has the power “to such an extent as is reasonable” to regulate the conduct of pupils when they are offsite. This is significant in cyber bullying which often takes place out of school but which can impact very strongly on the school life of those pupils involved.
- Confiscation of mobile phones when they are being used to cause a disturbance in class, around school or as an accessory to bullying is included within the act.
- Cyber bullying can be a criminal offence under the Protection from Harassment Act 1997, Communications Act 2003 and the Public Order Act 1986. The age of criminal responsibility in the UK starts at 10 years old.
- Think before you send – whatever you send can be made public very quickly and could stay online forever.
- Do not retaliate or reply to someone who is bullying you.
- Save the evidence – learn how to keep records of offending messages or pictures and contact a member of staff if you need advice.



Virtual Learning Environment (Moodle)

The purpose of the Burscough Priory Science College’s Virtual Learning Environment is to deliver electronic learning. This “Responsible Use” statement will help protect pupils, staff and the school by clearly stating what is acceptable and what is not.

- Accessing the Virtual Learning Environment with an account other than the one assigned to you is strictly forbidden. The school can determine when accounts are logged on.
- Contributions must be civil and respectful.
- No disruptive, offensive or abusive behaviour; contributions must be constructive and polite, not disrespectful or contributed with the intention of causing trouble.
- No unlawful or objectionable content: unlawful, harassing, defamatory, abusive, threatening, harmful, obscene, profane, sexually oriented, racially offensive or otherwise objectionable material is not acceptable.
- If you use multiple logins for the purpose of disrupting or annoying other students, you may have action taken against your account.
- No spamming or off-topic material: Burscough Priory Science College does not allow the submission of the same or very similar contributions many times. Please do not re-submit your contribution to more than one discussion, or contribute off-topic material in subject-specific areas.

- No advertising or posting promotional material unless prior agreement has been made with the school.
- No inappropriate (e.g: vulgar, offensive etc) language and names or impersonation.



Wireless Usage

The wireless network supports 802.11a/b/g/n/ac connections. Users must ensure that their equipment matches this configuration. The School does not guarantee connectivity with all manufacturers' equipment. Limited technical support is offered and faults should be reported to ICT Support: itsupport@bpsc.co.uk.

Use of the wireless network may be provided as a trust privilege to students in Year 11, however students in other years may be permitted access for educational usage when agreed with the ICT Support Department.

- The school does not guarantee that the wireless service will be fault free and will, where practicable, give advance notice of disruption or service suspension and will try to keep such disruption to a minimum.
- The wireless service must be used in accordance with the School's Acceptable Use Policy and Guidelines including the Computer Misuse Act (1990)
- It is prohibited to use the wireless service to attempt unauthorised access to another computer or network devices (on or off site).
- Activity and hardware on the wireless service can be monitored. The School will monitor and check the wireless service network traffic for the purpose of ensuring the correct operation of the network, fair allocation of resources and other lawful purposes.
- Equipment connected to the wireless service is your responsibility. You will be held accountable for any misuse identified on your Wireless equipment. You are responsible for all network traffic originating from that wireless connection.
- Any reports or incidents received or monitored by the school, regarding unauthorised or illegal access will result in immediate disconnection from the wireless, pending further investigations. Where necessary, information will be passed on to the relevant authorities.
- Wireless service users must take all practical steps to make sure that equipment connected to the wireless service is virus free and adequately secure. Prohibited devices discovered shall lead to the permanent termination of the wireless service
- The wireless service is a shared resource, any activity or software that uses excessive bandwidth (for example, continuous downloading and/or uploading), inhibits or interferes with other users is prohibited.
- The School reserves the right to disconnect users from, and make changes to the wireless service at any time without notice.

Student Name: _____ Form: _____



I do hereby agree to and acknowledge Burscough Priory Science College's Acceptable Use and Cyber Safety Policy Statement. I understand I may have my right or privilege to use systems provided by the school revoked or suspended if I engage in or support inappropriate activity.

Student Signature: _____

Parent/Carer Signature: _____ Date: _____