

# Homerton Hospitality Acceptable Use Policy

---

The “network” is taken to mean all parts of the network infrastructure, including any College owned PCs, wiring and active network equipment whether wired or wireless.

## Misuse of the network

The network shall not be used for:

1. Unlawful, fraudulent, criminal or otherwise illegal activities
2. Sending, receiving, publishing, posting, distributing, disseminating, encouraging the receipt of, uploading, downloading, recording, reviewing, streaming or using any material which is offensive, abusive, defamatory, indecent, obscene, unlawful, harassing or menacing or a breach of the copyright, trademark, intellectual property, confidence, privacy or any other rights of any person – this should be taken to include pornography and the use of peer-to-peer software
3. Sending or uploading unsolicited emails, advertising or promotional materials, offering to sell any goods or services, or conducting or forwarding surveys, contests or chain letters
4. Knowingly or negligently transmitting or uploading any electronic material (including, without limit, files that contain viruses, corrupted files, or any other similar software or programmes) which is known or likely to cause, interrupt, damage, destroy or limit the functionality of any computer software, hardware or telecommunications equipment owned by Homerton College or any other Internet user or person
5. Activities that invade another’s privacy, cause annoyance, inconvenience or needless anxiety to any person
6. Activities that are in breach of any other third party’s rights, including downloading, installation or distribution of pirated software or other inappropriately licensed software, deletion of any author attributions, legal notices or proprietary designations or labels in any file that is uploaded, falsification of the origin or source of any software or other material
7. Anything that may disrupt or interfere with Homerton College’s network or services or cause a host or the network to crash
8. Launching “denial of service” attacks; “mailbombing” attacks; or “flooding” attacks against a host or network
9. Granting access to your network services to others not residing at the College
10. Making excessive use of, or placing unusual burdens on, the network, for example by sending or receiving large volumes of email or excessively large email attachments
11. Circumventing the user authentication or security process of a host or network
12. Creating, transmitting, storing or publishing any virus, Trojan, corrupting programme or corrupted data
13. Monitoring or recording the actions of any other person on the network without their knowledge or any person or thing outside of the College including, without limitation, any public highway or roadway or another person’s home or business premises
14. Collecting, streaming, distributing or accessing any material that you know, or reasonably should know, cannot be legally collected, streamed, distributed or accessed.

## Filtering Lists

The Hospitality service is subscribed to Internet filtering lists in order to aid the prevention of network misuse. The lists are categorised by an external company and updated on a regular basis. The filter lists are not exhaustive and should be used as a guide to the type of content that is not permitted.

**By logging on to the network you agree to abide by this policy and understand that any breaches of the terms will result in disconnection from the network (with or without notice as the College IT Department deems appropriate).**