# Wi-Fi Network Acceptable Use Policy

West Dean Technical Resources

## Policy statement

This policy sets out the responsibilities and required behaviours for anyone granted permission to use Wi-Fi Networks provided by Technical Resources.

## Purpose and scope

The TR Wi-Fi Network Acceptable Use Policy provides everyone (e.g. students, staff, visitors, contractors, third parties) with clear and consistent guidance and rules for the use of College Wi-Fi networks. The policy is designed to protect the integrity, confidentiality and availability of the Technical Resources IT services whilst promoting responsible and ethical behaviour when using these resources.
Non-compliance with this policies puts people's personal and work data, and the College as a whole at risk. A breach of information security may result in damage to you, our students, or your colleagues through the loss of control over personal data or confidential data, identity theft, fraud or financial loss. Breaches to this policy also put the College at risk of cyber-threats, legal action and regulatory penalties.

Our IT systems log most aspects user interaction and these logs can be used in the event of complaint, investigation or subject access requests.

## Responsibilities for every user

Everyone is collectively responsible for protecting our College IT resources. Your responsibility includes keeping your usernames and passwords safe and secure.

Part of being careful about acceptable use of College IT resources involves being able to identify and avoid the risks from malware, ransomware, and phishing attacks.

If you get an email from anyone or anywhere that you are not sure about, please remember:

- Don't open any attachments
- Don't click on any links in the email

If you are in any doubt, or you are worried that the email might be malicious or inappropriate, please seek assistance immediately from the IT Helpdesk.

You are prohibited from using any College-provided IT System directly or indirectly for the download, creation, manipulation, transmission or storage of:

- any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- unlawful material or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
- any material which promotes terrorism or violent extremism, or which seeks to radicalise individuals to such causes;
- material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the College or a third party;
- material which promotes discrimination on the basis of age, sex, sexual orientation, race, religion or belief, pregnancy, marital/civil partnership status, gender reassignment, or disability;
- material with the intent to defraud or which is likely to deceive a third party;
- material which advocates or promotes any unlawful act;
- material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party;
- material that brings the College into disrepute.