



Wi-Fi Acceptable Use Policy

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for safeguarding children, all users must understand the boundaries and expectations when using the school Wi-Fi. Users are expected to use Wi-Fi safely, lawfully and responsibly, and to take reasonable steps to protect devices, data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list. All users are reminded that technology use should be consistent with the school ethos, relevant policies and the law.

1. The school provides Wi-Fi for education use and limited personal use. Staff have access to Wi-Fi through their school devices. With permission, staff may have access to the school Wi-Fi on their personal devices where appropriate. Visitors and staff have access to limited Guest Wi-Fi access. Wi-Fi use is monitored by the school Senior Leadership Team, ICT Lead and Primary Technologies.
2. Use of the Wi-Fi falls under Ospringe CE Primary School Acceptable Use of Technology Policy (AUP), the child protection policy, behaviour policy/code of conduct, data protection/security policies and any other relevant policies. All pupils, staff, visitors and volunteers using the Wi-Fi must comply with these expectations.
3. The school reserves the right to limit, restrict, withdraw or manage Wi-Fi access where necessary to maintain safeguarding, security, network reliability or fair use of network resources.
4. School owned information systems, including Wi-Fi, must be used lawfully. I understand that the Computer Misuse Act 1990 makes it a criminal offence to gain unauthorised access to computer material, gain unauthorised access with intent to commit or facilitate further offences, or modify computer material without authorisation.
5. I will take reasonable steps to ensure that any personal device connected to school Wi-Fi is appropriately secure, for example by using security updates, antivirus protection where appropriate, and secure passwords/PINs.
6. I will respect system security and will not share passwords, Wi-Fi access details or security information. I will not attempt to bypass school security, filtering or monitoring systems, or download unauthorised software, applications or files.
7. I will not use school Wi-Fi to access, create or share illegal or harmful content, compromise another person's safety or privacy, interfere with systems, or breach relevant school policies.
8. I will not use school Wi-Fi to access, store, send or share confidential, personal or safeguarding information unless this has been specifically authorised and is in line with school data protection and safeguarding procedures.

9. Staff using school Wi-Fi on personal devices remain subject to the staff behaviour policy/code of conduct, Staff AUP, mobile phone/smart device policy, data protection expectations, and relevant safeguarding and disciplinary procedures.
10. The school takes reasonable and proportionate steps to manage the security of its Wi-Fi service. However, no wireless or internet service can be guaranteed to be free from all risk. Where personal devices are permitted to connect to the school Wi-Fi, users do so at their own discretion and are expected to keep their devices secure. Any concerns about Wi-Fi security, filtering, monitoring or device safety should be reported to the DSL or identified technical contact.
11. I will report any online safety concerns, filtering breaches, security concerns, or access to inappropriate materials to the Designated Safeguarding Lead, Amanda Ralph or identified technical contact as soon as possible. If I have any queries about safe behaviour online, I will speak to the DSL or identified technical contact (Primary Technologies).
12. I understand that activity carried out through school Wi-Fi may be monitored and recorded to check policy compliance, protect systems and help keep users safe, including where the Wi-Fi is accessed using a personal device. This does not mean that the school can monitor other activity or information held on the personal device. Monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
13. If the school suspects that unauthorised or inappropriate use, unacceptable behaviour, a data protection concern, a safeguarding concern or criminal activity may have taken place, access may be restricted or withdrawn and the concern may be managed in line with relevant school procedures. Where appropriate, this may include informing the DSL, Data Protection Officer, headteacher/manager, employer/organisation, LADO or police.

I have read, understood and agreed to comply with Ospringe CE Primary School Wi-Fi acceptable Use Policy.

Name

Signed:Date (DDMMYY).....