Theale Church of England Primary School

Acceptable Use of ICT Policy

Whilst exciting and beneficial both in and out of the context of education web-based resources, in particular, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised WBC and school staff.
In appropriate circumstances, as directed by the head teacher, authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice.

- All users must take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally.
- All users must be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies.
- No communications device, whether school provided or personally owned, may be used for the bullying or harassment of others in any form.
- No applications or services accessed by users may be used to bring the school, or its members, into disrepute.
- All users have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others.
- All users have a duty to respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.
- All users have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
- All users have a duty to protect their passwords and personal network logins, and should log off the network when leaving workstations unattended. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

- All users should use network resources responsibly. Wasting staff effort or networked resources, or using the resources in such a way so as to diminish the service for other network users, is unacceptable.
- All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- All users should be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to check and/or confiscate personal technologies such as mobile phones.
- All users should understand that the AUP is regularly reviewed and consistently enforced.
- All staff must sign the Staff AUP and a copy be kept on file.

Accidental or deliberate access to inappropriate material
Staff must be vigilant when navigating the internet at school, especially when pupils are present.

If inappropriate materials are accidentally found, these should be reported to a member of staff, or the headteacher. Any inappropriate materials such as pictures or text which are brought into school will be treated as a disciplinary action.

Accidental or deliberate access to illegal material
If filters are correctly set, it should not be possible to access illegal materials. School staff are authorised by the head teacher to deactivate filters in order to access resources for the purposes of education or training. In such circumstances, members of staff are responsible for the materials they access and ensuring the physical security of ICT equipment while filters are deactivated. If illegal material is accessed, escalation of the incident will be necessary.

Inappropriate use of email or other technologies
If inappropriate e-mails are sent or received, these should be reported to a member of staff or the headteacher. Any inappropriate use of e-mail or other technologies for the purpose of cyber bullying will be treated as a disciplinary action.

Illegal use of email and other technologies
Illegal use of email and other technologies will be dealt with initially within school but may be escalated to appropriate external agencies.

Deliberate misuse of the network
Monitoring of the network is in place and the sanctions which will apply to deliberate misuse. (for example, hacking, virus propagation or circumventing safety controls). If networks have been used for illegal activity, the incident should be escalated accordingly.

Bullying or harassment using technologies
Bullying or harassment is not acceptable in any circumstance, via any means, and will be dealt with in the same way as those documented in established anti-bullying policies. It may also be necessary to involve appropriate external agencies, depending on the severity of the event.

Sexual exploitation using technologies
This is a serious offence, and will require escalation to appropriate external agencies as necessary.

Laptops

A laptop issued to a member of staff or parent remains the property of the school (see laptop use policy). Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

Reviewed: Spring 2021

Next Review: Spring 2024