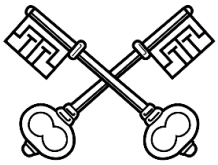

RADLEY

Use of IT Policy

November 2023

Use of IT Policy

ICT presents tremendous opportunities, but is not without its own difficulties. To that end, Radley aims to put sensible constraints on the use of ICT whilst endeavouring to maximise the educational and operational value available from new technologies.

We anticipate that most adults and pupils will own, and often carry, devices which have access to the Internet and therefore have the ability to perform most common digital tasks such as research, word processing, analysis, communication, content delivery and the like. Increasingly such devices operate autonomously much of the time.

Policy for the use of Information and Communication technology at Radley College

1. Legal, Decent, Honest: Anything created, stored, sent or processed using ICT must be both socially and legally acceptable.
2. Duty of Care: Radley College provides resources and services in pursuit of the aims of the institution; it has a Duty of Care to its pupils, employees, visitors and their families. All users are reminded of their responsibilities to each other and the requirement that the College should not be brought into disrepute.
3. Rules and Policies: The use of technology is subject to the same Code of Conduct, rules and policies as other aspects of Radley life. (e.g. as apply to defamation, obscenity, pornography, harassment, bullying, radicalisation, sexual exploitation or terrorism).
4. Safeguarding, cyber-bullying and Prevent: ICT represents a powerful lever for harm as well as for good. All users are required to report any concerns.
5. Network Security. Under no circumstances should a user be culpable for any action or omission which might compromise the security or privacy of ICT systems (e.g. hacking, failure to maintain anti-virus protection, lax password security).
6. Privacy and Data Protection: Under no circumstances should a user be culpable for any action or omission which might compromise Data which might be considered sensitive, confidential, subject to Data Protection or subject to intellectual property rights. Extensive guidance is provided in the College Data Processing Guidelines and in the Privacy Policy.
7. Audio, Video: The use of audio, imagery or video is subject to the College's Images Policy
8. Oversight and Search: The College reserves the right to investigate any abuse of digital resources where reasonable suspicion exists, and to withdraw the right to use and access such resources if abuse is identified.
9. Disciplinary Action: All users are advised that a breach of this policy may be treated as a breach of their contract with the College, and hence subject to disciplinary action.

Further guidance on the use of IT at the College

Users have access to technologies that have both positive and negative potential. The College encourages the use of technology in an academic, pastoral and operational context and recognises its growing importance in sport, social and leisure activities.

Given these facts, it is important that the use of technology is monitored and managed appropriately within the College environment and that users are appropriately trained and educated. The following measures seek to ensure this is the case:

1. Concerns and Reporting: Any issues or concerns about the use of technology should be reported to the College IT Help Desk, the IT Systems Manager or the Director of Digital Strategy as seems appropriate. Such issues will be escalated through normal management channels as appropriate. All users are encouraged to pass on any pastoral concerns about the abuse of technology to a member of the Pastoral Team. Safeguarding issues will be passed to the DSL.
2. eSafety: Online Safety is addressed in many ways: initially through Shell Computer Science lessons; the PSHE curriculum; CPD; via relevant talks and other channels (intranet, email, Social Prayers, etc). All users should be aware of the dangers of both the internet and of social media and endeavour to remain up-to-date with changes to the challenges and threats of the digital world.
3. CPD: The Director of Digital Strategy will brief adults on a regular basis about any particular concerns with regards to the use of technology in the school. Training is made available through an online resource focusing on key applications used within the organisation. Any requests for specific training should be addressed through the Director of Digital Strategy.
4. Filtering: The Designated Safeguarding Lead and Safeguarding Governor are responsible for monitoring the effective implementation of filtering software and of patterns of online use on the College network. They will be aided by the Director of Digital Strategy and IT Systems Manager.
5. Safeguarding: The DSL and Pastoral Team are trained regularly in safeguarding; such training specifically covers eSafety, with the DSL taking overall responsibility for the management of the safeguarding implications of technology, including the risks of radicalisation and sexual exploitation. As part of their safeguarding duties, dons are asked to keep a close eye on the use of technology both in and beyond the classroom. Form Masters and Tutors in particular should monitor the nature and extent of the use of technology by pupils and ensure that concerns are raised with parents as appropriate.
6. Communication with parents: The College regularly communicates with parents and include within that advice and guidance on matters of technology. Any individual concerns will be shared with parents, in the first instance by the Tutor.
7. Feedback and Student Voice: the use of technology within the school from pupils' perspective is regularly discussed on SMAC (Senior Master's Advisory Committee) and the Director of Digital Strategy attends those meetings when necessary.
8. Digital Resources Guidelines for the creation and development of Digital Resources are available on the College intranet.
9. Social media guidelines for the use and management of social media are available on the College intranet.
10. Hardware and Software. Pupils are provided with a device in the Shell year, further advice on hardware and software provision and specification should be sought via the IT Help Desk.

11. Works, Projects and Events. Developments of a significant nature should always be referred to the Director of Digital Strategy and the IT Systems Manager to ensure that digital provision and support is adequate and that digital opportunities are not missed.
12. Restrictions: Mobile Device Management software is used to provide appropriate restrictions to devices leased by the College to pupils. In appropriate circumstances, access to Digital Resources may be restricted by the Director of Digital Strategy or the IT Systems Manager. Similarly, in appropriate circumstances, Tutors may restrict pupils' access to technology.
13. Manners and Etiquette: users should avoid having their heads down in technology as they walk around campus and they should value human contact and conversation over what is on the screen. All users should know when to put a device down and when to put a device away; they should avoid using devices in Chapel, during meals and in social environments where conversation, discussion and debate should be valued. It is good practice to shun technology in the final half-hour before bedtime.
14. Security: Advice on password security is given to all users. Multi-Factor Authentication is a requirement of all users as implemented by the IT Systems Manager. Regular phishing campaigns are conducted to keep users familiar with vulnerabilities that may be exploited by outside organisations, and helps form part of the training provided to staff.

The digital world can often seem complex and change comes at a rate that is often challenging. That said, all users are cautioned that ignorance remains a poor excuse. If in doubt, further guidance should be sought and users are advised to err on the side of caution.