Student acceptable use policy

Blessed Edward Oldcorne Catholic College

1. Introduction and aims

ICT is an integral part of the way our college works, and is a critical resource for students, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the college.

However, the ICT resources and facilities our college uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of college ICT resources for students,
- Establish clear expectations for the way all members of the college community engage with each other online
- Support the college's policy on data protection, online safety and safeguarding
- Prevent disruption to the college through the misuse, or attempted misuse, of ICT systems

.

Breaches of this policy may be dealt with under our behaviour policy.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2020
- Searching, screening and confiscation: advice for colleges

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the college to use the ICT facilities
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the college to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the college's ICT facilities by any member of the college community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the college's ICT facilities includes:

- Using the college's ICT facilities to breach intellectual property rights or copyright
- Using the college's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the college's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the college, or risks bringing the college into disrepute
- Sharing confidential information about the college, its students, or other members of the college community
- Connecting any device to the college's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the college's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the college's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the college
- Using websites or mechanisms to bypass the college's filtering mechanisms

This is not an exhaustive list. The college reserves the right to amend this list at any time. The headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the college's ICT facilities.

4.2 Sanctions

Students who engage in any of the unacceptable activity listed above may face disciplinary action in line with the college's policies on behaviour and safeguarding.

Sanctions could include removal of IT privileges including revoking network and email passwords and not being allowed to use the college IT systems for a defined period of time.

5. Monitoring of college network and use of ICT facilities

The college reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The college monitors ICT use in order to:

- Obtain information related to college business
- Safeguard students
- Investigate compliance with college policies, procedures and standards
- Ensure effective college and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Students

6.1 Access to ICT facilities

- “Computers and ICT equipment in the college are available to students only under the supervision of staff”
- “Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff”
- “Students will be provided with an account linked to the college’s network and G Suite account.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education’s guidance on searching, screening and confiscation, the college has the right to search students’ phones, computers or other devices for pornographic images or any other data or items banned under college rules or legislation.

The college can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the college’s rules.

6.3 Unacceptable use of ICT and the internet outside of college

The college will sanction students, in line with the behaviour policy if a student engages in any of the following **at any time** (even if they are not on college premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the college’s policies or procedures

- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the college, or risks bringing the college into disrepute
- Sharing confidential information about the college, other students, or other members of the college community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the college's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Insulting members of staff

7. Data security

The college takes steps to protect the security of its computing resources, data and user accounts. However, the college cannot guarantee security. Students who use the college's ICT facilities should use safe computing practices at all times.

7.1 Passwords

All users of the college's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Students who disclose account or password information may face disciplinary action.

7.2 Software updates, firewalls, and anti-virus software

All of the college's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the college's ICT facilities.

Any personal devices using the college's network must all be configured in this way.

7.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the college's data protection policy.

7.4 Access to facilities and materials

All users of the college's ICT facilities will have clearly defined access rights to college systems, files and devices.

These access rights are managed by Mr Edmunds.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert a member of staff immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access.

8. Internet access

8.1 Students

- Wifi is available in all areas of the college
- Students will be given access when they join the college and this will be revoked when they leave
- Students are not to use their phones to access the internet using their own personal mobile data. Students found using their phones on the college site to access the internet will be dealt with via the college behaviour policy and mobile phone policy

9. Monitoring and review

The Headteacher and Mr Edmunds monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the college.

This policy will be reviewed every year.

The governing board is responsible for approving this policy.

10. Related policies

This policy should be read alongside the college's policies on:

- E safety
- Safeguarding and child protection
- Behaviour
- Data protection
- Remote learning
- Mobile phone policy