Staff Acceptable Use Policy
Blessed Edward Oldcorne Catholic College

Approved by: Full Governing Body **Date**: September 2020

Last Reviewed : September 2022

Next review due by: September 2023

Data security

In addition to responsibilities outlined in this document staff have a legal requirement to keep personal data securely and to only process it for lawful purposes as defined under GDPR 2018.
Further details of these responsibilities can be found in:
Data Protection Policy 2018
Privacy Notice – staff 2018
Privacy Notice – students 2018
Privacy Notice- parents 2018

1. Purpose

This Acceptable Use Policy is aimed at encouraging responsible behaviour and good practice. It has been created with the view to:

1.1 Ensure compliance and enforcement of relevant legislation which include but is not limited to the Computer Misuse Act and GDPR legislation.

1.2 Ensure the safety and integrity of students, staff and others.
1.3 Prevent damage to the College and its physical property.

2. Policy Statement

2.1 Blessed Edward Oldcorne Catholic College reserves the right to amend this Acceptable Use Policy, at anytime, without notice. It is your responsibility to ensure that you are up to date with such changes.
2.2 This Acceptable Use Policy replaces and supersedes all previous versions.

3. Electronic mail (e-mail)

3.1 All members of staff will be provided with email services for college related communication.

3.2 Caution should be exercised when sending confidential information via e-mail.

3.3 The transmission of confidential information via e-mail to unauthorised persons is strictly prohibited. Where there is a need to send personal data it must be password encrypted. If the e-mail contains data categorised as sensitive as defined by GDPR the DPO must give permission before this is sent.

3.4 The use of e-mail for personal purposes is permitted but must be reasonable and not include personal or sensitive data.

3.5 While Blessed Edward Oldcorne Catholic College respects the privacy of staff, where there is reason for concern or an operational need, the College reserves the right to monitor, delete, change passwords and intercept e-mail communication.

3.6 Any e-mail communication made must not bring the College into disrepute; this includes anything libellous, defamatory or criminal.

3.7 Pupils and parents must be contacted via College e-mail. Pupils must never be contacted via personal e-mail

4. Internet Access

4.1 All Internet access is logged for the purposes of maintaining standards of security and acceptable use.

4.2 Attempts to access inappropriate websites or websites which attempt to bypass filtering systems constitute a breach of this Acceptable Use Policy.

4.3 Inappropriate websites referred to in 4.2 include, but are not limited to any site which contains:

- Pornographic Material (of either a legal or illegal nature).
- Material which incites hatred or discrimination.
- Material which promotes illegal activity.
- Material which is in breach of the Copyright Designs and Patents Act 1998.
- Material which is degrading to persons or groups.

4.4 Staff are required to report any website that they become aware of, which is not filtered, that is deemed inappropriate as per the criteria stated within.

4.5 Staff should refrain from downloading large files during school hours as this may affect the quality of service for other users.

While Blessed Edward Oldcorne Catholic College uses sophisticated filtering technology and takes all precautious to ensure that users only access appropriate material, it is not possible to guarantee that unsuitable material will be inaccessible. Neither Blessed Edward Oldcorne Catholic College or staff can accept liability for the material accessed, or any consequences of such access.

4.6 Staff must take care when using social networking websites, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children. You must not allow any pupil to access personal information you post on a social networking site. In particular:

- You must not add a pupil to your 'friends list'.
- You must ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to

a ‘Friends only’ level of visibility.

• You should avoid contacting any pupil privately via a social networking website, even for college related purposes.

• You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the College – even if their online activities are entirely unrelated to the College.

• Unless authorised to do so, you must not post content on websites that may appear as if you are speaking for the College.

• You should not post any material online that can be clearly linked to the College that may damage the College’s reputation.

• You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

5. Network Access

5.1 Staff logins must only be used by the member of staff that they are issued to. Liability remains with the logged in user.

5.2 Allowing another person to use your login is a severe breach of this Acceptable Use Policy and contravenes GDPR legislation.

5.3 Passwords must never be divulged to anyone at any time.

5.4 If it is suspected that a password has been compromised it must be changed immediately.

5.5 Staff will not attempt to download or install software onto the network or IT Equipment.

5.6 It is prohibited to copy any software or inappropriate material on to the network.

5.7 Staff will not store confidential material on network areas which are accessible to persons who do not have clearance to access such material.

5.8 Staff should understand that the right is reserved to remotely monitor and intercept network activity.

6. Legislation

6.1 All network users are bound by current relevant legislation. The applicable laws (as amended) include, but are not limited to:

- GDPR 2018
- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1998
- Criminal Justice Act 1988
- Defamation Acts 1952 and 1996
- Freedom of Information Act 2000
- Human Rights Act 1998
- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1988
- Protection from Harassment Act 1997
- Public Order Act 1986
- Race Relations Amendment Act 2000

- Telecommunications Act 1984
- Sex Discrimination Act 1986
- Regulation of Investigatory Powers Act (RIPA) 2000

6.2 Staff should understand that any attempt to bypass the College, or other network security systems, including the introduction of viruses or applications of a destructive nature could lead to prosecution.

6.3 Where it is believed that a member of staff is in breach of legislation appropriate action will be taken.

7. ICT Equipment and Suites

7.1 Staff may not move or authorise any person to move any ICT Equipment.

7.2 Staff may not pass on any ICT Equipment to any other person. It must first be passed back to ICT Support and then reissued.

7.3 Any equipment issued to staff remains the property of the College and must be returned upon request.

7.4 Upon termination of employment at the College all equipment must be returned.

7.5 Staff are responsible for all equipment issued to them and must take reasonable precautions to protect such equipment, including complying with insurance requirements of securing equipment at all times.

7.6 Staff are responsible for all equipment and use of workstations by students during their lessons in ICT Suites. Their department will be billed for any associated damage.

8. Additional Systems

8.1 Members of staff may have access to additional systems which include, but are not limited to: SIMs, Mintclass, Edutrack, Finance Software, SEN database, Exam Software and Attendance Software.

8.2 These systems require additional passwords. It is the responsibility of the member of staff to ensure that their password has basic complexity to it and that their password is only known by them.

9. Sanctions

If this Acceptable Use Policy is breached, staff will be subject to sanctions which may include, but are not limited to:

- Disciplinary procedures.
- Temporary or permanent restriction of network access
- Temporary or permanent revocation of network rights
- Restriction to or denial of access to ICT Suites
- Investigation under the Regulation of Investigatory Powers Act (RIPA) 2000.