BLESSED EDWARD OLDCORNE
CATHOLIC COLLEGE

E-Safety Policy

Approved by:	Full Governing Body	**Date:**	October 2023
Last reviewed on:	October 2022		
Next review due by:	October 2023		

Staff Responsibilities

Assistant Headteacher (ICT):	**Mr P Edmunds**
Designated Safeguard Lead:	**Miss K Mason**
Deputy Safeguard:	**Mr G McClarey, Mrs S Thomas, Mrs K Ennis**
IT Manager:	**Mr B Pain**

Contents

……

1. Aims

Our College aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole College community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for Colleges on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the College's ICT systems and the internet (appendix 2)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the College.

3.3 The designated safeguarding lead

Details of the College's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The DSL delegates responsibility for online safety in College to the Assistant Headteacher with responsibility for whole College ICT. This role will:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the College
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the College behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in College to the headteacher and/or governing body

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at College, including terrorist and extremist material
- Ensuring that the College's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the College's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy

- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the College's ICT systems and the internet (appendix 2), and ensuring that pupils follow the College's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the College's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the College's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The College will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The College works in partnership with National Online Safety. This organisation produce an app which we encourage all parents to download. This app contains the latest information on online threats and equips parents with the necessary information on what maintain an up-to-date knowledge of cyber threats. National Online Safety regularly sends push notifications to the parental app with the latest online safety news.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the College behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The College will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The College also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the College will follow the processes set out in the College behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the College will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Sexting

Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages.

They can be sent using mobiles, tablets, smartphones, laptops - any device that allows you to share media and messages.

Creating or sharing explicit images of a child is illegal, even if the person doing it is a child. A young person is breaking the law if they:

- take an explicit photo or video of themselves or a friend
- share an explicit image or video of a child, even if it’s shared between children of the same age
- possess, download or store an explicit image or video of a child, even if the child gave their permission for it to be created.

Any cases of sexting will be passed onto the DSL to investigate and possible referrals to the police.

6.4 Child on child Abuse

Children can abuse other children. This is generally referred to as child on child abuse and can take many forms. This can include (but is not limited to) bullying (including cyberbullying); sexual violence and sexual harassment; physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm; sexting and initiating/hazing type violence and rituals.

Any allegations of child on child abuse will be recorded on My Concern after the allegation has been investigated and dealt with accordingly.

Students who are victims, perpetrators and any other child affected by child on child abuse will be supported by the relevant agencies and networks linked to our College.

6.5 Sexual Violence and sexual harassment

Sexual violence and sexual harassment can occur online and offline (both physically and verbally), and are never acceptable. All victims will be taken seriously and offered appropriate support.

Sexual harassment refers to unwanted conduct of a sexual nature that occurs online or offline. Sexual harassment violates a child’s dignity and makes them feel intimidated, degraded or humiliated, and can create a hostile, sexualised or offensive environment.

Sexual harassment includes:

- Sexual comments.
- Sexual "jokes" and taunting.
- Physical behaviour, such as deliberately brushing against another pupil.
- Online sexual harassment, including non-consensual sharing of images and videos and sharing sexual images and videos (often known as sexting), inappropriate comments on social media, exploitation, coercion and threats – online sexual harassment may be isolated or part of a wider pattern.

Sexual Violence

Children can, and sometimes do, commit sexual violence. The DfE uses the definitions of sexual violence provided in the Sexual Offences Act 2003:

- Rape: A person (A) commits an offence of rape if: he intentionally penetrates the vagina, anus or mouth of another person (B) with his penis, B does not consent to the penetration and A does not reasonably believe that B consents.
- Assault by Penetration: A person (A) commits an offence if: s/he intentionally penetrates the vagina or anus of another person (B) with a part of her/his body or anything else, the penetration is sexual, B does not consent to the penetration and A does not reasonably believe that B consents.
- Sexual Assault: A person (A) commits an offence of sexual assault if: s/he intentionally touches another person (B), the touching is sexual, B does not consent to the touching and A does not reasonably believe that B consents.

Consent is given when a person agrees by choice, and has the freedom and capacity to make that choice. Consent may be given to one kind of sexual activity but not another. Consent can be withdrawn at any time and each time an activity occurs.

Harmful sexual behaviour may include:

- Using sexually explicit words and phrases.
- Inappropriate touching.
- Sexual violence or threats.
- Full penetrative sex with other children or adults.

The Brooks sexual behaviours traffic light tool will help the College make decisions about whether sexual behaviour is harmful or natural.

As a College we should:

- Make it clear that sexual violence and sexual harassment are never acceptable and will never be tolerated – it is not an inevitable part of growing up.
- Not dismiss or tolerate sexual violence or harassment as "banter" or "part of growing up".
- Challenge behaviour such as grabbing bottoms, breasts and genitalia. Tolerating such behaviours risks normalising them – they are potentially criminal acts.
- Understand that sexual violence and sexual harassment can be driven by wider societal factors, such as everyday sexist stereotypes and language.

Where a child discloses safeguarding allegations of a sexual nature against another pupil in the same setting, the DSL should refer to the West Midlands Safeguarding Children procedures website (section 3.3) and seek advice from the Family Front Door or Community Social Worker before commencing its own investigation or contacting parents. This may mean, on occasions, that the school is unable to conduct its own investigation into such incidents. All such incidents will be recorded using our child protection recording forms.

Reports of incidents of sexual violence or sexual harassment will be responded to in line with Part 5 of Keeping Children Safe in Education 2018 and the DfE guidance 'Sexual violence and sexual harassment between children in schools and colleges'.

6.6 Examining electronic devices

College staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the College rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of College discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the College complaints procedure.

7. Acceptable use of the internet in College

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the College's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the College's terms on acceptable use if relevant.

Use of the College's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff (where relevant), volunteers, governors and visitors to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in College

Pupils may bring mobile devices into College, but are not permitted to use them at any point during the College day.

Any use of mobile devices in College by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the College behavior policy, which may result in the confiscation of their device.

9. Staff using work devices outside College

Staff members using a work device outside College must not install any unauthorised software on the device and must not use the device in any way which would violate the College's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside College. Any USB devices containing data relating to the College must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the College will respond to issues of misuse

Where a pupil misuses the College's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the College's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The College will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Illegal or inappropriate activities and related sanctions

The College believes that the activities listed below are inappropriate in a school context (those in bold are illegal) and that users should not engage in these activities whenusing school equipment or systems (in or out of school).

Users shall not visit Internet sites, make,post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal – The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act1986)**
- pornography
- promotion of any kind ofdiscrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which maybe offensive to colleagues or breaches the integrity of the ethos of the College or brings the College into disrepute

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The Assistant Principal (ICT) and or Network Manager will undertake online safety training at least every 2 years. They will also update their knowledge and skills on safeguarding at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

A designated ICT support staff member will provide weekly monitoring reports to the Assistant Headteacher (ICT). Any immediate threats to safety will be passed on immediately.

Only the Headteacher or Assistant Headteacher (ICT) can give authorisation to monitor or not monitor staff computers. The nature of some staff roles will require confidential computer use, monitoring in these circumstances may not be appropriate, it will be at the discretion of the named roles in determining this action.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the College’s ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the College’s ICT systems and accessing the internet in College, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher’s permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the College’s network using someone else’s details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into College:

- I will keep it switched off and in my bag until I leave the College campus.

I agree that the College will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the College’s ICT systems and internet responsibly.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the College’s ICT systems and internet when appropriately supervised by a member of College staff. I agree to the conditions set out above for pupils using the College’s ICT systems and internet, and for using personal electronic devices in College, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the College's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the College's ICT systems and accessing the internet in College, or outside College on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the College's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the College's network using someone else's details

I will only use the College's ICT systems and access the internet in College, or outside College on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the College will filter and monitor the websites I visit, **with notification.**

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside College, and keep all data securely stored in accordance with this policy and the College's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the College's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in College?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the College's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the College's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the College's ICT systems?	
Are you familiar with the College's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident