# TRINITY CATHOLIC SCHOOL

Online Safety Policy

**Signed by Head of School:**

## Contents



Date of implementation – May 2020

Date of next review – May 2021

# 1. Aims

Trinity Catholic School 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 school 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 (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Head of Schools and school staff
- [Relationships and sex education
- 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.

Maintained schools and academies that follow the National Curriculum insert:

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

Academies, including free schools, if applicable, add/amend: This policy complies with our funding agreement and articles of association.

# 3. Roles and responsibilities

## 3.1 The Interim Executive Board

The Interim Executive Board has overall responsibility for monitoring this policy and holding the Head of School to account for its implementation.

The Interim Executive Board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

If applicable, add: The governor who oversees online safety is [name/role of individual].

All governors will:

- Ensure that they have read and understand this policy

## 3.2 The Head of School

The Head of School is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout Trinity Catholic School.

## 3.3 The designated safeguarding lead

Details of Trinity Catholic School's DSL [and deputy/deputies] are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head of School in ensuring that staff understand this policy and that it is being implemented consistently throughout Trinity Catholic School
- Working with the Head of School, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with Trinity Catholic School behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head of School and/or Interim Executive Board

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 school, including terrorist and extremist material
- Ensuring that Trinity Catholic School'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 Trinity Catholic School's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with Trinity Catholic School 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
- 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 Trinity Catholic School behaviour policy

This list is not intended to be exhaustive.

### 3.6 Parents

Parents are expected to:

- Notify a member of staff or the Head of School of any concerns or queries regarding this policy

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

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

### 3.7 Visitors and members of the community

Visitors and members of the community who use Trinity Catholic School'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 3).

## 4. Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

From September 2020 **all** schools will have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

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

*By the **end of secondary school**, they will know:*

- *Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online*
- *About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online*
- *Not to provide material to others that they would not want shared further and not to share personal material which is sent to them*
- *What to do and where to get support to report material or manage issues online*
- *The impact of viewing harmful content*
- *That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*

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

Trinity Catholic School will use assemblies and PSHCE sessions 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

Trinity Catholic School will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Edulink. This policy will also be shared with parents via Trinity Catholic School website

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head of School.

# 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

## 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.

Trinity Catholic School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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).

Trinity Catholic School 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, Trinity Catholic School will follow the processes set out in Trinity Catholic School behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, Trinity Catholic School 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 Examining electronic devices

School 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 Trinity Catholic School 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 school 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 Trinity Catholic School complaints procedure.

## 7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of Trinity Catholic School's ICT systems and the internet. Visitors will be expected to read and agree to Trinity Catholic School's terms on acceptable use if relevant.

Use of Trinity Catholic School'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, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

## 8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but they must be off and in their bags during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by Trinity Catholic School

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

## 9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate

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 school

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. Using online resources to support home learning

Home or distanced learning via an online platform (e.g. Edulink, Moodle or Microsoft Teams) may be required in the following circumstances:

- School closure (either directed from government, caused by weather or health and safety issues on the school site)
- Health issues resulting in low attendance on the school site

This section of the policy is implemented alongside:

(a) The Child Protection and Safeguarding Policy
(b) The Staff Code of Conduct Policy

All of which reference the dangers, expectations and monitoring of using online platforms to deliver home learning.

Trinity Catholic School has reviewed and updated its child protection and safeguarding, online safety and acceptable use policies, ensuring that all staff involved in virtual teaching or the use of technology to contact pupils are briefed on best practice and any temporary changes to policy / procedures.

When selecting a platform for online / virtual teaching, the school should satisfy itself that the provider has an appropriate level of security. Trinity Catholic School has consulted with Warwickshire County Council to ensure that the chosen online communication platform meets wider guidelines and expectations.

*This means that senior leaders should:*

▪ *review and amend their online safety and acceptable use policies to reflect the current situation*
▪ *ensure that all relevant staff have been briefed and understand the policies and the standards of conduct expected of them*
▪ *have clearly defined operating times for virtual learning*
▪ *consider the impact that virtual teaching may have on children and their parents/ carers / siblings*
▪ *determine whether there are alternatives to virtual teaching in 'real time' – e.g., using audio only, prerecorded lessons, existing online resources*
▪ *be aware of the virtual learning timetable and ensure they have the capacity to join a range of lessons*
▪ *take into account any advice published by the local authority,or their online safety / monitoring software provider*

Staff should use school devices and contact pupils only via the pupil school email address / log in. This ensures that Trinity Catholic School's filtering and monitoring software is enabled.

In deciding whether to provide virtual or online learning for pupils, senior leaders should take into account issues such as accessibility within the family home, the mental health and wellbeing of children, including screen time, the potential for inappropriate behaviour by staff or pupils, staff access to the technology required, etc. Virtual lessons should be timetabled and senior staff, DSL and / or heads of department should have a rota of monitoring in place and have the ability to any virtual lesson at any time – the online version of entering a classroom.

If staff are engaging in online learning via video conference, they should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents. The following points should be considered:-

▪ think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred

▪ staff and pupils should be in living / communal areas – no bedrooms

▪ staff and pupils should be fully dressed

▪ filters at a child's home may be set at a threshold which is different to the school

▪ resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary. Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / pupil consent is needed and retention / storage. If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately. Staff, parent and pupil AUPs should clearly state the standards of conduct required.

*This means that staff should:*

▪ *adhere to Trinity Catholic School's policies*
▪ *be fully dressed*
▪ *ensure that a senior member of staff is aware that the online lesson / meeting is taking place and for what purpose*
▪ *avoid one to one situations – request that a parent is present in the room for the duration, or ask a colleague or member of SLT to join the session*
▪ *only record a lesson or online meeting with a pupil where this has been agreed with the head teacher or other senior staff, and the pupil and their parent/carer have given explicit written consent to do so*
▪ *be able to justify images of pupils in their possession*

*This means that adults should not:*

▪ *contact pupils outside the operating times defined by senior leaders*
▪ *take or record images of pupils for their personal use*
▪ *record virtual lessons or meetings using personal equipment (unless agreed and risk assessed by senior staff)*
▪ *engage online while children are in a state of undress or semi-undress*

## How Trinity Catholic School will respond to issues of misuse

Where a pupil misuses Trinity Catholic School's ICT systems or internet, we will follow the procedures set out in our policies on [behaviour and ICT and internet acceptable use – adapt according to what policies you have]. 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 Trinity Catholic School'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/staff code of conduct]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

## 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 DSL [and deputy/deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety 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

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every academic year by the safeguarding team.  At every review, the policy will be shared with the Interim Executive Board.

## 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
- ICT and internet acceptable use policy

Date of implementation – May 2020

Date of next review – May 2021