

# Trinity School

## Online Safety Policy



### **DOCUMENT REVIEW**

GOVERNOR APPROVAL DATE: January 2020

COMMITTEE RESPONSIBLE: Education

AUTHOR: T Battley

NEXT REVIEW DATE: January 2022



## Table of Contents

1. Aim .....	3
2. Legislation and guidance .....	3
3. Roles and responsibilities .....	3
4. Educating students about online safety .....	5
5. Cyberbullying .....	6
6. Acceptable use of the internet in school .....	7
7. Staff using work devices outside of school .....	7
8. How the school will respond to issues of misuse .....	7
9. Training .....	8
10. Links with other policies .....	8



## 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, 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 cyberbullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE'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 cyberbullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

## 3. Roles and responsibilities

### 3.1 The governing board

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 school's ICT systems and the internet

### 3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school in accordance with the below sections.



### **3.3 The Designated Safeguarding Lead (DSL)**

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged onto the school's system (CPOMS) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary

Our Designated Safeguarding Lead is Mrs Tara Battley.

### **3.4 SLT member responsible for ICT**

There is a member of the Senior Leadership Team with responsibility for ICT. They are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting full security checks and monitoring the school's ICT
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

### **3.5 All staff**

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet as detailed in our Acceptable Use Policy
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school behaviour policy



### 3.6 Parents

Parents are expected to:

- Notify the Designated Safeguarding Lead or the headteacher of any concerns or queries regarding this policy
- Ensure that they and their child have read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Parents can seek further guidance on keeping children safe online via the below organisations and websites:
- Trinity School Safeguarding - <https://www.trinitysevenoaks.org.uk/1643/safeguarding>
- 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 the 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 of the school's ICT systems and the internet as detailed in our Acceptable Use Policy.

## 4. Educating students about online safety

Students will be taught about online safety as part of the PSHE (Personal, Social, Health and Economic) and Computer Science curricula.

By the end of secondary school, students 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 imprisonment
- 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. The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

## 5. Cyberbullying

### 5.1 Definition

Cyberbullying 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.

### 5.2 Preventing and addressing cyberbullying

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

The school will actively discuss cyberbullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyberbullying with their tutor groups and the issue will be addressed in assemblies.

All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support students, as part of safeguarding training.

In relation to a specific incident of cyberbullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the 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.

### 5.3 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 students' 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 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 students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

## **6. Acceptable use of the internet in school**

All students, parents/carers and staff are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the 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 students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

## **7. Staff using work devices outside of school**

Staff members using a work device outside of school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as detailed in our Acceptable Use Policy.

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.

## **8. How the school will respond to issues of misuse**

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our Child Protection and behaviour policies. The action taken will depend upon the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the 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/code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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



## 9. Training

All new staff members will receive safeguarding training as part of their induction which will include online safeguarding issues including cyberbullying 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 online training, emails, bulletins and staff meetings).

The DSL and deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every two 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 online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

## 10. Links with other policies

This online safety policy is linked to our:

- Child Protection Policy
- Behaviour Policy
- Staff disciplinary procedures/Code of Conduct
- Acceptable Use Policy (for staff)
- Acceptable Use Agreement (for students/parents/carers)