

# Online Safety Policy

Golborne St Thomas' CE J & I School



**Last reviewed on:** November 2021

**Next review due by:** November 2022

**A journey in faith, arriving with hope.**

**St. Thomas' School vision:**

**To ensure the children are highly valued by all members of the school community.**

St. Thomas' creates a culture of high aspirations by making the school the heart of the community. We aim to develop a culture of curiosity and creativity by unleashing our children's God-given potential to make a difference in our locality and beyond.

Our parents, staff and governors see and understand the individual talents of each pupil and the opportunities provided. We openly celebrate and reward children's successes and achievements.

**To inspire all children through a broad, balanced and engaging curriculum enabling every child to succeed.**

We create an ethos where everyone is an explorer and an active participant. Children are challenged and encouraged to thrive in all areas. Our aim is to nurture talent and ensure children are equipped to live life in all its fullness.

Children experience a wide range of high quality lessons and enrichment activities daily. We recognise that children are naturally curious; therefore, child-led learning is developed through their questions.

**To nurture children's wellbeing to ensure healthy mind, body and spirit.**

At St. Thomas' values are at the heart of all we do. We provide a safe, supportive environment which empowers children to grow and develop their self-worth, self-esteem and self-respect. Our unique learners are resilient and are willing to take big risks to make big leaps.

Values are actively promoted, modelled, and celebrated by all. Our inspiring curriculum and pastoral care teaches children the importance of healthy lifestyles: physically, mentally and spiritually.

## **Contents**

1. Aims .....	3
2. Legislation and guidance .....	3
3. Roles and responsibilities .....	3
4. Educating pupils about online safety .....	5
5. Educating parents about online safety .....	5
6. Cyber-bullying .....	6
7. Acceptable use of the internet in school .....	7
8. Virtual Teaching/Home learning .....	7
9. Pupils using mobile devices in school .....	7
10. Staff using work devices outside school .....	7
11. How the school will respond to issues of misuse .....	7
12. Training .....	7
13. Monitoring arrangements .....	8
14. Links with other policies .....	8
Appendix 1: School acceptable use agreement (pupils, staff and parents/carers) .....	9

---

## 1. Aims

Our 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 headteachers 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.

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

## 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.

The governing 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).

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.

### 3.3 The designated safeguarding lead

Details of the school's DSL [and 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 headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- › Working with the headteacher, computing leader and other staff, as necessary, to address any online safety issues or incidents
- › Ensuring that any online safety incidents are logged 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 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 headteacher and/or governing board

This list is not intended to be exhaustive.

### **3.4 The computing leader**

The computing leader 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 the 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 the school's ICT systems on a fortnightly 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 the 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
- › Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- › Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with policy
- › Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the 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 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 school'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](#)

- › 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.

## 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

This new requirement includes aspects about online safety. As such, we've added these expectations in italics below.

In **Key Stage 1**, pupils will be taught to:

- › Use technology safely and respectfully, keeping personal information private
- › Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- › Use technology safely, respectfully and responsibly
- › Recognise acceptable and unacceptable behaviour
- › Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- › *That people sometimes behave differently online, including by pretending to be someone they are not.*
- › *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- › *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- › *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- › *How information and data is shared and used online*
- › *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

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

The school will use e-safety lessons 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 school will raise parents' awareness of internet safety in letters or other communications home. This policy will also be shared with parents.

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

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

## **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 school 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 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. Class teachers will discuss cyber-bullying with classes, 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).

The 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, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, 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.

### **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 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 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 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 the school's ICT systems and the internet (appendices 1). 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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreement in appendix 1

## 8. Virtual teaching/ Home learning

When face to face teaching is not viable in the event of a full/partial school closure, for example during the global pandemic from Covid-19, virtual teaching will take place in line with the school's virtual teaching policy. Home learning will be available via Seesaw (an online learning journal) where class teachers will post lessons and work daily for the children to access. Once pupils have completed their work, teaching staff will provide feedback with the following comments: objective met; objective nearly met, can you.../next time, can you...; or, objective not met yet, can you.../next time, can you...

## 9. Pupils using mobile devices in school

Pupils should not bring mobile phones into school. In the event that children do have their phone for travelling to/from school, they should hand their phone into the school office on arrival. This can then be collected at the end of the day.

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

## 10. 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 the school's terms of acceptable use.

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. Any USB devices containing data relating to the school must be encrypted.

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

Work devices must be used solely for work activities.

## 11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our 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 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 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.

## 12. 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 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.

### **13. Monitoring arrangements**

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

This policy will be reviewed every year by the computing leader. At every review, the policy will be shared with the governing board.

### **14. Links with other policies**

This online safety policy is linked to our:

- › Safeguarding and Child Protection Policy
- › Behaviour Policy
- › Social Media Policy
- › Data protection Policy.
- › Complaints procedure



## Appendix 1: Acceptable Use Agreement

### Rules for Responsible PC Use

-----

The school has installed computers and Internet access to help our learning.

These rules will keep everyone safe and help us be fair to others.

-----

- I will only access the system with my own login and password, which I will keep secret
- I will not access other people's files
- I will only use the computers for school and home work
- I will not bring in CD's or other computer media from outside school unless I have been given permission
- I will ask permission from a member of staff before using the Internet
- I will only e-mail people I know, or my teacher has approved
- The messages I send will be polite and responsible
- I will not give my home address or telephone number, or arrange to meet someone unless my parent, carer or teacher has given permission
- I will report any unpleasant material or messages sent to me
- I understand my report would be confidential and would help protect other pupils and myself
- I understand that the school may check my computer files and may monitor the Internet sites I visit