Taverham High School
An 11-18 Academy
Inspire | Empower | Achieve

# Online Safety Policy

**Purposes**

- Safeguard and protect all children and staff;
- Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice;
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community;
- Have clear structures and processes that can be implemented to deal with online abuse such as online bullying and ensure that these structures run in conjunction with procedures in other relevant school policies;
- Ensure that all members of the school community are aware that unlawful or unsafe online behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

| | |
|---|---|
| Responsible Staff Member | GYS |
| Committee to Review | Full Governing Board |
| Ratification date by Committee | Spring 2025 |
| Review Due | Spring 2027 |

# Contents

## 1. Introduction and Overview

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
- 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 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 main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms

Conduct:

- personal online behaviour that increases the likelihood of, or causes, harm.

The online safety policy is referenced within other school policies (e.g. Safeguarding

and Child Protection policy, Anti-Bullying policy).

The online safety policy will be reviewed biennially or when any significant changes occur with regard to the technologies in use within the school. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- online abuse learning - nspcc.org.uk/child-abuse-and-neglect/online-abuse
- bullying learning - nspcc.org.uk/child-abuse-and-neglect/bullying
- child protection learning - nspcc.org.uk/child-protection-system

As a School we recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using THSs network and devices
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

## 2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the computing curriculum. This covers a range of skills and behaviours appropriate to their age and experience.
- will remind students about their responsibilities through the pupil ICT Code of Conduct/ Acceptable Use Agreement.
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright.
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.

By the end of secondary school, pupils 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
- Some of the threats posed to networks, including malware and phishing
- What is meant by phishing and how to keep data safe from phishing attacks
- Precautions which can be taken to keep data safe from hackers including anti-malware software, firewalls, user access levels, passwords and encryption

Staff training

This school will ensure :

- up-to-date training is available to staff on online safety issues and the school's online safety education program.
- It provides, as part of the induction process, all staff (including those on university/college placement and work experience) with information and guidance on the Online Safety Policy and the school's ICT Code of Conduct/ Acceptable Use Agreement.)

Parent/Carer awareness and training

This school:

- provides information for parents/carers for online safety on the school website.

In this school:

- Our IT provider conducts strict monitoring and application of the online safety policy, including the ICT Code of Conduct and a differentiated and appropriate range of sanctions. Support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre Helpline, CEOP, Police, Child Net) in dealing with online safety issues
- Monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school.
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, CEOPs.

## 3. Managing IT and Communication Systems

Internet access, security and filtering

In this school:

- We follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision. By doing so, we will ensure that the school networks are kept secure and protected from internal and external threats.

E-mail

This school:

- We provide staff with an email account for their professional use and make clear personal email should be through a separate account.
- We use anonymous e-mail addresses, for example head@, office@.
- We will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.

Pupils' email:

- We use school provisioned pupil email accounts that can be audited.
- Pupils are taught about the online safety and etiquette of using e-mail both in school and at home.

Staff email:

- Staff will use their school provisioned e-mail systems for professional purposes.
- Access in school to external personal email accounts may be blocked.
- Staff will never use email to transfer staff or pupil personal data outside of the school unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The school web site complies with statutory DfE requirements
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs of pupils published on the web do not have full names attached.

- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Social networking

Staff, Volunteers and Contractors:

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- The use of any school approved social networking will adhere to the ICT Code of Conduct/Acceptable Use Policy.
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our pupil ICT Code of Conduct/Acceptable Use Policy.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through our parental ICT Code of Conduct/ Acceptable Use Policy and additional communications materials when required.
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or

violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

## 4. Data Security

Management Information System access and data transfer

- We follow the guidance from the Information Commissioner's Office to ensure that we comply with our responsibilities to information rights in school. We will ensure that we regularly check that we are compliant.

## 5. Equipment and Digital Content

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- Staff sign the school's ICT Code of Conduct/Acceptable Use Policy and this includes a clause on the use of personal mobile phones/personal equipment.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications this is covered under the parental permission agreement.

## 6. Cyber-bullying

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.)

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. Members of the computing department will discuss cyber-bullying with pupils across the whole key stage 3 cohort, during discrete computing lessons and across the whole key stage 4 cohort, during core computing lessons. 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. 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.

## 7. 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.

## 8. 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. 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 whilst they are on school property.

## 9. 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 policies on (Behaviour, Anti-bullying and ICT and internet acceptable use). 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 disciplinary procedures/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.

## 10. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour and rewards policy
- Anti-Bullying Policy
- ICT and internet acceptable use policy
- Data protection policy and privacy notices

## Appendix 1: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff and governors

Name of staff member/trustee:

When using the school's ICT facilities and accessing the internet in school, or outside school 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 (or create, share, link to or send such material)
- ☒ Use them in any way which could harm the school'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, or connect unauthorised hardware or devices to the school's
- ☒ network
- ☒ Share my password with others or log in to the school's network using someone else's details
- ☒ Share confidential information about the school, its pupils or staff, or other members of the
- ☒ community
- ☒ Access, modify or share data I'm not authorised to access, modify or share
- ☒ Promote private businesses, unless that business is directly related to the school

- ✓ I confirm that I have read the school's ICT policy in full.
- ✓ I understand that the school will monitor the websites I visit and my use of the school's ICT facilities
- ✓ and systems.
- ✓ I will take all reasonable steps to ensure that work devices are secure and password-protected when
- ✓ using them outside school, and keep all data securely stored in accordance with this policy and the
- ✓ school'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 school's ICT systems and internet responsibly, and ensure that pupils in my care
- ✓ do so too.

Signed (staff member/trustee):

Date:

## Appendix 2: Acceptable use agreement for pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT facilities and accessing the internet in school, I will not:

- ☒ Use them for a non-educational purpose
- ☒ Use them without a teacher being present, or without a teacher's permission
- ☒ Use them to break school rules
- ☒ 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 any semi-nude or nude images, videos or livestreams, even if I have the consent of the
- ☒ person or people in the photo
- ☒ Share my password with others or log in to the school's network using someone else's details
- ☒ Bully other people

- ✓ I understand that the school will monitor the websites I visit and my use of the school's ICT facilities
- ✓ and systems.
- ✓ 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 school's ICT systems and internet responsibly.
- ✓ I understand that the school can discipline me if I do unacceptable things online, even if I'm not in
- ✓ school when I do them.

Signed (pupil):

Date:

Parent/carer agreement:

- ✓ I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff.
- ✓ I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date: