

Online Safety

Date of Policy Issue	Oct 2024
Date of Policy Review	Oct 2025
Name of Responsible Manager	Deputy Headteacher
Governors' Sub-Committee	Welfare & Guidance
Statutory/Non-Statutory	Non-statutory
Published to Website (Internal/External)	External

Aims

1.0 Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2.0 Legislation and guidance

2.1 This policy is based on the Department for Education's (DfE's) 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 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 policy also takes into account the National Curriculum computing programmes of study.

3.0 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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;

- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is the Chair of Governors.

All governors will:

- Ensure 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 (appendix 3)**
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

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 (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

1. Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
2. Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
3. Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
4. Working with the IT support company to make sure the appropriate systems and processes are in place
5. Working with the headteacher, IT support company and other staff, as necessary, to address any online safety issues or incidents
6. Managing all online safety issues and incidents in line with the school's child protection and safeguarding policies.
7. Ensuring that any online safety incidents are dealt with appropriately in line with this policy
8. Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

9. Updating and delivering staff training on online safety
10. Liaising with other agencies and/or external services if necessary
11. Providing reports on online safety in school to the headteacher and/or governing board
12. Undertaking annual risk assessments that consider and reflect the risks children face
13. Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 **IT Support Company (Medhurst)**

The IT Support Company are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are reported to the DSL immediately and dealt with appropriately in line with this 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.

3.5 **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 (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing through the School Safeguarding reporting systems.

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers 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/carers 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](#)
- Parent resource sheet – [Childnet](#)

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 able to access this policy via the school website.

4.0 Educating pupils about online safety

Pupils will be taught about online safety as part of the Computer Science and Personal Development curriculum:

All schools have to teach:

- [Relationships and sex education and health education](#) in secondary schools

Pupils 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
- 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 that 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 that 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
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

All schools:

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5.0 Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be available to parents/carers via the school's website.

Online safety will also be covered during parents' information evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online
- The Personal Development Curriculum and Computer Science Curriculum are available on our website for Parents to see the content

If parents/carers have any queries or concerns in relation to online safety or this policy, they should be raised with the headteacher and/or the DSL by contacting dsl@toynbee.hants.sch.uk

6.0 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.

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. Assemblies around the use of social media and cyber bullying are held. The teaching of Online Safety and specifically Cyber Bullying is a thread throughout the spiral curriculum of Personal Development 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, and other subjects where appropriate.

All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents/carers so 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's behaviour and anti-bullying 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 report the incident and provide the relevant material to the police and children's services as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (as outlined in the Behaviour Policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

The Behaviour Policy outlines the protocol for conducting a search of pupils. In all cases, authorisation from a member of the Senior Leadership Team must be sought and two members of staff must be present.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it must be referred to the Headteacher/DSL/the Senior Leadership Team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- The Toynbee Behaviour Policy
- The Substance Misuse and Drugs Education Policy

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

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Toynbee school recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Toynbee school will treat any use of AI to bully pupils in line with our behaviour policy and anti-bullying policy.

7.0 Acceptable use of the internet in school

All pupils, staff, volunteers and governors are expected to sign that they have read and understood the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

More information is set out in the acceptable use agreements in appendices 1 to 3.

8.0 Pupils using mobile devices in school

The school will follow the [DFE: Mobile phones in schools - February 2024](#) guidance, adopting the “never used, seen or heard” principle. This will be communicated at least annually to pupils, parents and staff. Pupils are permitted to bring their mobile phone to school; however, it must not be visible or audible at any time and must be kept in a school bag or locker.

Staff will be expected to consistently enforce this policy by reporting pupils that are seen using their mobile phones to the Pastoral Team. Staff should not use their own mobile phone for personal reasons in front of pupils throughout the school day.

Parents will be informed when their child has been reported for using their mobile phone.

The school will issue sanctions, as outlined in the Behaviour Policy, when a pupil is in breach of the mobile phone policy. When a mobile phone is seen by a member of staff, it is deemed a prohibited item and as a result staff will follow the process for Searching, Screening and Confiscation as outlined in the Behaviour Policy. For the purposes of this policy, Mobile Phones includes any device used to communicate (e.g. electronic watches), MP3 players, tablets and headphones/ear pods.

9.0 Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Not sharing the device among family or friends
- Making their device available to the IT Support Company as required.

Staff members must not use the device in any way that would violate the school’s terms of acceptable use, as set out in appendix 2.

If staff have any concerns over the security of their device, they must seek advice from the IT Support Company.

10.0 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 the Behaviour Policy and Pupil Acceptable Use document. 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police and/or Local Authority Designated Officer (LADO).

11.0 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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL 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.

12.0 Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on through the school's internal reporting systems and CPOMS.

This policy will be reviewed every year by the Welfare and Guidance Committee. At every review, the policy will be shared with the governing board.

13.0 Links with other policies

This online safety policy is linked to the following policies which can be found on our website:

<https://www.toynbee.hants.sch.uk/our-school/policies/>

- Child protection Policy
- Safeguarding policy
- Behaviour policy
- Anti-Bullying Policy
- The Substance Misuse and Drugs Education Policy
- Data Protection policy and Privacy notice
- Complaints procedure

The following appendices should be read in conjunction with this policy

Appendix 1 – Pupil Acceptable Use Agreement

Appendix 2 – Staff Acceptable Use Policy

Appendix 3