The Telford Park School

Ensuring Excellence

Online Safety Policy

Approved: December 2023

Date for review: December 2024

Online Safety Policy

Policy Name:	Online Safety Policy
Headteacher:	Mrs H Rigby
School Standards Committee:	Mr S Mirza
Date:	December 2023
Date for policy review:	December 2024

Contents

Online Safety Policy

1. Aims

The Telford Park School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing standards of teaching and learning. There are several controls in place to ensure the safety of pupils and staff.

The range of issues classified within online safety are considerable, however they can be categorised into four areas of risk:

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

The Telford Park 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, including mobile and smart technology (which we refer to as 'mobile phones')
- 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'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.

Maintained schools and academies that follow the National Curriculum insert:

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

This policy applies to all members of the school community including staff, pupils, volunteers, parents, carers, and visitors who have access to and are users of schools' digital technology systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers regarding the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

3. Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

The Educational Advisory Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Educational Advisory 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 by accepting the Telford Park acceptable use agreement termly on their device.

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

The Headteacher

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

The Designated Safeguarding Lead

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:

Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents

Managing all online safety issues and incidents in line with the school child protection policy

Ensuring that adequate online filtering and monitoring software is in place (Senso, Smoothwall) which effectively logs incidents in order of severity. Incidents must then be triaged 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 via CPOMS.

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 the schools governing body.

This list is not intended to be exhaustive.

The ICT Manager

The ICT manager is responsible for:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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 on a weekly basis

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Ensuring that any online safety incidents are logged via Senso and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately via CPOMS in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers (where using school hardware and systems)

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 by accepting the Telford Park acceptable use agreement termly, and ensuring that pupils follow the school's terms on acceptable use and the pupil code of conduct as detailed in the Behaviour Policy appendix a

Working with the DSL to ensure that any online safety incidents are logged via CPOMS 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

Responding appropriately in accordance with safeguarding procedures 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.

Parents and Carers

Parents and carers are expected to:

Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Ensure that their child has read, understood and agreed to the terms as set out within the pupil code of conduct relating to acceptable use of the school's ICT systems and the internet

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 resource sheet – Childnet International

Visitors and members of the community (where using school hardware and systems)

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 by accepting the Telford Park acceptable use agreement MS Form termly.

4. Educating pupils about online safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.

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.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships and sex education and health education in secondary schools

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

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**, 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
- 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)

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. Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

- The school will let parents 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

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.

Educating the wider community

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents
- The school website will provide online safety information for the wider community
- Work with feeder primary schools to enhance their online safety provision and the knowledge of transitioning pupils

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and anti-bullying 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. Teaching and support staff will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSHRE, 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.

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 report the incident and provide the relevant material to the police 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.

Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting in line with the DfE's latest guidance on searching, screening, and confiscation:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL or DDSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

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 is up to DSL or DDSL 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 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
- Our behaviour 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.

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 (pupil/staff code of conduct, acceptable use agreement). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant to their position.

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 and using school devices/via the school internet) to ensure they comply with the above using the school ICT filtering/monitoring software.

More information is set out in the acceptable use agreement and pupil/staff code of conduct.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but must have them switched off and in their bags. The school have adopted a 0 tolerance approach to mobile phones. The new mobile phone policy uses the slogan 'See it, Hear it, Take it'.

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

9. 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 – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device is locked when not in use

- Not sharing the device among family or friends
- Report any incidents concerning cyber security such as phishing to the ICT Manager

Staff members must not use the device in any way which would violate the school's terms of acceptable use or staff code of conduct.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT manager. *Note, the ICT Manager will be responsible for ensuring that any school device:*

- *Has an encrypted hard drive – 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*
- *Has anti-virus and anti-spyware software installed*
- *Has up to date operating systems by always installing the latest updates*

10. 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 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 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.

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).

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, 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 and can weigh up the risks
- 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 and DDSLs 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 via the pastoral/behaviour log and Senso monitoring system as appropriate.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Educational Advisory Board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Anti-bullying policy
- Behaviour policy (inclusive of pupil code of conduct, appendix a)
- CAT privacy notices
- Child on child abuse policy
- Child protection and safeguarding policy (plus appendix 1)
- Complaints policy
- Data protection policy
- ICT and internet acceptable use agreement
- PSHE and RSE policy
- Risk assessment policy
- Staff code of conduct
- Online Safety Risk Assessment

14. Appendix (Acceptable Use Agreement)

Appendix – Acceptable Use Agreement (Automatically generated termly for all users of ICT, must be accepted to use ICT systems and hardware)

Telford Park School Acceptable Use Agreement OF ICT Facilities & Devices

This computer/Laptop & system is owned by the school. This Acceptable Use statement helps to protect students, staff and the school by clearly stating what use of the ICT resources is acceptable and what is not. If any further clarification is required, please contact the Headteacher, DSL or ICT manager.

School computer and Internet use must be for educational purposes. Any doubt as to what constitutes educational use should be referred to the Headteacher.

- Network access must be made with the user's authorised account and password, which must not be given to any other person. When temporarily leaving a workstation, it should be locked. (Ctrl-Alt-Del or Windows L) to prevent unauthorised access.
- Any messages should be written responsibly and politely. Abuse of any kind is forbidden.
- Users are responsible for any messages they send and for contacts made.
- Any unpleasant or inappropriate content should be reported to ICT services or SLT.
- Caution should be exercised before giving out any personal details, or information about the school, over the network.
- Anonymous messages and chain letters are not permitted.
- Not all resources on the Internet are free. Users must be aware of copyright and intellectual property rights before distributing content or resources.
- Use for personal financial gain, gambling, political purposes, or advertising is not permitted.
- ICT security systems must be respected; they are there for the benefit of all users. Any attempt to bypass security systems is a serious offence.

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I understand that the computer/laptop remains the property of Telford Park School and that I am responsible for the safe keeping of the device.

I understand that I am liable for any damage to the device on or off site, and the school reserved the right to claim back any costs incurred to cover the repair/replacement of the device.

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.