Stamford Park
PRIMARY SCHOOL

# Online Safety Policy

| | |
|---|---|
| Agreed by the Governing Body in: | November 2023 |
| Review Date: | November 2024 |
| Review Schedule: | Annually |
| Person(s) Responsible: | Mike Smith |

# Online Safety Policy

## Our Aims

As a school, we aim 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.

## Application of this policy

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

## The four 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.

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

## 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 is informed by 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.

**Roles and responsibilities**

**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.

**The headteacher**

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

The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the dayto-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.

The headteacher and Online safety leader will receive regular monitoring reports from the Trafford IT services and SmoothWall teams.

**The designated safeguarding lead**

Details of the school's designated safeguarding lead (DSL) and deputies (Mrs Price, Ms Bogart and Mr Spinola respectively) are set out in our child protection and safeguarding policy.

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

- Supporting the Senior Leadership team and ICT Coordinator 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,

- Ensuring that any incidents of cyber-bullying within school are logged and dealt with appropriately in line with the school behaviour policy. The DSL and ICT Coordinator will support where possible in an advisory role with regards to any incidents that take place outside of school.
- Liaising with other agencies and/or external services if necessary,
- Take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)

This list is not intended to be exhaustive.

**The ICT coordinator**

The ICT coordinator (Edmund Reeves) and Online Safety lead (Michael Smith) are responsible for:

- Putting in place and understand 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. This is in line with the guidance given within the Keeping Children Safe In Education document.
- Reviewing all breaches of filter policies and acting if necessary on these breaches. This is done in Partnership with Trafford IT services and SmoothWall monitoring.
- Providing regular feedback on online safety in school to the DSL to remain proactive.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- 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.

**Parents**

Parents are expected to:

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

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

**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.

### Educating pupils about online safety

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

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.

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.

The school will use assemblies and focus days to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

### 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, both within school and outside of school, 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 within school and are encouraged to do so, including where they are a witness rather than the victim.

The school will discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal Development & Wellbeing and other subjects where appropriate.

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.

**Pupils using mobile devices in school**

Pupils may bring mobile devices into school but must leave them in the office and only collect them when leaving school.

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.

Watches are accepted as part of our School Uniform Policy, but these must be watches that do not allow pupils to communicate using the internet.

**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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

**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, bulletins and staff meetings).

**Published content and the school web site**

Editorial guidance will ensure that the school's ethos is reflected on the website, information is accurate, well presented and personal security is not compromised.

Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.

The school will ensure that content is accurate and appropriate.

- Photographs, videos and podcasts of school activities, alongside first names only, may be uploaded. This is in line with what may be shown on a classroom wall or school display and shared within our physical community.

**Publishing pupil's images and work**

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by members of the public viewing the website.

Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

The permissions will be requested as part of our home/school agreement.

**Appendix 1**

**EYFS and KS1 acceptable use agreement (pupils and parents / carers)**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: SUGGESTIONS FOR PUPILS AND PARENTS/CARERS

**When I use the school's ICT systems (like computers) and get onto the internet in school I will:**

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

**Appendix 2**

**EYFS and KS2 acceptable use agreement (pupils and parents / carers)**

## ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: SUGGESTIONS FOR PUPILS AND PARENTS/CARERS

**Name of pupil:**

**When I use the school's ICT systems (like computers) and get onto the internet in school I will:**

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

**I will not:**

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- 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
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

**If I bring a personal mobile phone or other personal electronic device into school:**

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**