Online Safety Policy
John T Rice Infant and Nursery School

2025

Reviewed: September 2025

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors, including clear oversight of filtering, monitoring and cybersecurity systems.
- 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'), generative AI and emerging technologies.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate, and to log, review and learn from incidents to strengthen practice.

2. 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, misinformation, disinformation, conspiracy theories, and AI-generated material (including deepfakes).
- **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.

3. Scope of the Policy

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, *Keeping Children Safe in Education (KCSIE 2025)*, 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
- 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, the Equality Act 2010, and the Education Act 2011. It also reflects the National Curriculum computing programmes of study.

This policy applies to all members of the John T Rice Infant and Nursery School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of school.

The school will deal with 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.

4. Roles and Responsibilities

Governors

- Approve the online safety policy and review its effectiveness.
- Receive regular information about online safety incidents and monitoring reports.
- Seek assurance that senior leaders and the DSL understand how filtering and monitoring systems work and are effective in practice.
- Ensure the school has completed the DfE "Plan technology for your school" self-assessment and acted on recommendations.
- Monitor the school's cyber resilience, including incident response and recovery planning.

Headteacher and Senior Leaders

- Hold overall responsibility for the safety (including online safety) of the school community.
- Ensure filtering and monitoring systems are regularly reviewed, tested in real-world conditions, and improved where weaknesses are identified.
- Ensure there is a cyber incident response plan and staff know how to escalate concerns.
- Ensure the Computing Lead and other relevant staff receive suitable training.
- Receive regular reports from the Online Safety Lead.

Online Safety Lead (DSL)

- Take day-to-day responsibility for online safety issues and policy development.
- Ensure staff are aware of reporting procedures for online incidents.
- Provide training and advice for staff.
- Liaise with external agencies as appropriate.
- Monitor and act upon alerts from filtering/monitoring systems.
- Ensure pupils are educated about misinformation, disinformation and safe use of emerging technologies including AI.

- Report regularly to the governing body.

Network Manager/Technical Staff (ATOM IT)

- Ensure the school's technical infrastructure is secure against misuse or attack.
- Ensure the filtering policy is applied, updated regularly, and not managed by one individual alone.
- Regularly monitor the use of networks/internet/digital technologies and report misuse.
- Test and evidence the effectiveness of filtering and monitoring systems.
- Detect and flag attempts to bypass filtering (VPNs, proxies).
- Contribute to the school's cyber resilience strategy, including recovery planning.

Teaching and Support Staff

Are responsible for ensuring that:

- Maintain awareness and have an up to date awareness of online safety matters and follow the current school online safety policy and practices.
- They have read, understood and signed the staff acceptable use policy/agreement.
- Report suspected misuse to the Headteacher/DSL.
- Use only official school systems for communications with pupils/parents.
- Embed online safety in teaching and curriculum delivery.
- Staff/ pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Model safe, responsible use of technology.

Pupils

- Use school digital technology systems responsibly, in line with acceptable use agreements.
- Report abuse, misuse or inappropriate materials.
- Understand online bullying and misuse and adopt safe online practices both in and out of school.
- Learn about misinformation, disinformation, and AI-generated content.

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. John T Rice Infant School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents are expected to sign an acceptable use agreement. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records

Parents/carers are expected to: Notify a member of staff or the headteacher of any concerns or queries regarding this policy. Ensure they and their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet and that parents/carers have understood and signed the terms of acceptable use. 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

Community/Outside Users

- Community/outside users who access school systems or programmes as part of the wider *John T Rice Infant and Nursery School* provision will be expected to sign an acceptable use agreement.

5. Education and Training

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the John T. Rice 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. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Receive a planned, progressive online safety curriculum across computing, PSHE and other subjects, including assemblies.
- Children will be taught the SMART rules and the principles of safe behaviour online.
- Pupils should be taught to critically evaluate online content, including misinformation, disinformation and AI-generated content.
- Pupils should learn about plagiarism, copyright and responsible research.
- Pupils should be helped to understand the need for safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through newsletters, the website, workshops, and campaigns such as Safer Internet Day.

Staff and Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Receive regular training in online safety, updated in line with KCSIE guidance.
- Are trained on boundaries in digital communications, recognising and responding to misinformation, disinformation, and misuse of AI.

- The Computing Lead attends external training and disseminates updates in staff meetings/ training sessions.
- It is expected that some staff will identify online safety as a training need within the performance management process.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by Governor services.
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

6. Cyber-bullying

- Defined as intentional, repeated online harm where there is an imbalance of power. For example, through social networking sites, messaging apps or gaming sites. (See also the school behaviour policy).
- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes as part of RHE and computing lessons. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- Staff receive training on its prevention and response. In relation to a specific incident of cyber-bullying, the school will follow the school processes. 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.

7. Technical Infrastructure, Filtering and Monitoring

Managed by ATOM IT with oversight from school leaders. ATOM IT oversees the technical infrastructure and equipment within the school but it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school as suggested below. ATOM IT is aware and follows John T Rice Infant and Nursery School's online policy.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements There will be regular reviews and audits of the safety and security of school technical systems.

- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school/academy technical systems and devices.
- The "master/administrator" passwords for the school/academy systems, used by the Network Manager (or other person) must also be available to the Headteacher and staff where necessary and kept in a secure place
- ATOM IT is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users by Securly. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. Under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet.
- John T Rice Infant and Nursery School has provided enhanced/differentiated user-level filtering allowing different filtering levels for different ages/stages and different groups of users – staff/pupils
- Technical staff at ATOM IT regularly monitor and record the activity of users on the school technical systems – any breaches of illegal activity are flagged via email from Securly to the HT
- It is the responsibility of the HT to follow these up and liaise with ATOM IT

- Systems tested regularly and reviewed using the DfE self-assessment tool.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the Head teacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- There is provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place for removable media such as memory sticks/memory cards to use as storage. Memory sticks and removable storage are not permitted at John T Rice Infant and Nursery School.
-

8. Staff Use of Devices outside of 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).
- 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.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software and keeping operating systems up to date by always installing the latest updates.
- Staff members must not use the device in any way which would violate the school's terms of acceptable use.
- Work devices must be used solely for work activities.

9. Mobile Technologies

Mobile technology devices such as iPads are school owned. All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. Personal mobile devices such as smart phones are not to be used for school business purposes.

- The school acceptable use agreements for staff, pupils and parents/carers also includes the school mobile technologies.

10. Responding to 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 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.

Review of this Policy

This online safety policy has been developed by the Computer Lead along with the Headteacher and Governing Body.

11. Review and Monitoring

- Approved by governors (Autumn term 2025).
- Monitored by Governing Body, Headteacher and Computing Lead.
- Reviewed annually, or sooner if there are changes to KCSIE or incidents.
- Next review due Autumn 2026.
- Serious incidents reported to external agencies (LA Safeguarding Officer, LADO, Police).

12. Monitoring the Impact of the Policy

- Logs of reported incidents.
- Monitoring data from ATOM IT and Securly.
- Internal network monitoring data.
- Surveys/questionnaires of pupils, parents, staff.