Online Safety Policy

John T Rice Infant and Nursery School

2024

Reviewed: September 2024

Aims

1. Our 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

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

Scope of the Policy

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.

This policy applies to all members of the *John T Rice Infant and Nursery* 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 John T Rice Infant and Nursery School.

John T Rice Infant and Nursery 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.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within John T. Rice Infant and Nursery School

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the *Full Governing Body* receiving regular information about online safety incidents and monitoring reports.

Headteacher/Principal and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility is everyone's responsibility.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the Computing Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

The Online Safety Lead is also the Designated Safeguarding Lead, the headteacher. This will be done in conjunction with the computing Lead. They will:

- take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies/documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place

- provide training and advice for staff
- liaise with the Local Authority/relevant body
- liaise with school technical staff
- receive reports of online safety incidents and creates a log of incidents to inform future online safety developments examples of which are found at the end of this policy
- meet regularly with the *Governing Body* to discuss current issues, review incident logs and filtering/change control logs
- attend relevant meetings of *Governors*
- report regularly to Senior Leadership Team

The incidents will be dealt with in line with the school procedure for safeguarding in school.

Network Manager/Technical staff

The John T. Rice Infant and Nursery School's network is managed by the company ATOM IT and the school works alongside ATOM IT to ensure all online safety measures are carried out.

Those with technical responsibilities are responsible for ensuring:

- that the John T. Rice Infant and Nursery School technical infrastructure is secure and is not open to misuse or malicious attack
- that John T. Rice Infant and Nursery School meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/ Senior Leadership
- that monitoring software/systems are implemented and updated as agreed in John T Rice Infant School policies
- ATOM IT manage the Securly filtering and monitoring system. They are responsible for creating the security policies
- Securly monitoring sends a daily update to the HT with a report of access attempts

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use policy/agreement

- they report any suspected misuse or problem to the Headteacher for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the Online Safety Policy and acceptable use policies
- 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

Designated Safeguarding Lead

Is trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

Students/Pupils:

- are responsible for using the *John T. Rice Infant School* digital technology systems in accordance with the acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and have some understanding of online bullying and misuse
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *John T Rice Infant School* online safety policy covers their actions out of school, if related to their membership of the school

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.

Policy Statements

Education - 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: (A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited

- Key online safety messages should be reinforced as part of a planned programme of assemblies and activities.
- Children will be taught the SMART rules (see appendix 1) and these are referred to at the beginning of every online lesson.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- 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.

Training

Education – 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:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents/carers online safety session
- High profile events/campaigns e.g. Safer Internet Day

Education & Training – Staff/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:

- Online safety training will be made available to staff where needed and also linked to Safeguarding training. This will be regularly updated and reinforced.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The computing lead will receive regular updates through attendance at external training by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings/training sessions.
- The computing lead will provide advice/guidance/training to individuals as required.

Training – Governors

Governors/Directors 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).

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.)

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. 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

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.

Technical – infrastructure/equipment, filtering and monitoring

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
- 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.

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).
- 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.

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.

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 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.

Schedule for Development/Monitoring/Review:

This online safety policy was approved by the Governors at the strategic development committee meeting:	*Autumn term 2024* *16.10.2023*
The implementation of this online safety policy will be monitored by the:	*The Governing Body* *The Head teacher* *The Computing Lead*
Monitoring will take place at regular intervals:	*At least each term or regularly as needed*
The Board of Governors will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*At each full Governing Body Meeting once a term.*
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Autumn 2025*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA Safeguarding Officer, LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering done by ATOM IT.
- Monitoring logs on Securly
- Internal monitoring data for network activity
- Surveys/questionnaires of
  - students/pupils
  - parents/carers
  - staff