E-Safety Policy 2017

Our Vision

John T Rice Infant & Nursery School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communication technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, John T Rice Infant & Nursery School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and young people while on the school premises.

Related Documents:
Acceptable Use of the Internet Policy
Safeguarding Policy
Data Protection Policy
Behaviour Policy
Anti-bullying Policy
Computing Policy

Publicising e-Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website.
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated.
- Post relevant e-Safety information in all areas where computers are used
- Provide e-Safety information to parents via the website and when necessary through newsletters at the beginning of each term.

Roles and Responsibilities

The Head and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our school. The role of e-Safety coordinator has been allocated to Kerry Scotney, they are the central point of contact for all e-Safety issues and will be responsible for day to day management. All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly.
- Accept responsibility for their use of technology.
- Model best practice when using technology.
- Report any incidents to the e-Safety coordinator using the school procedures.
- Understand that network activity and online communications can be monitored, including any personal and private communications made via the school network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action.

Physical Environment / Security

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly
- Central filtering is provided by Fortinet and managed by AtomIT.
- All staff and students understand that if an inappropriate site is discovered it must be reported to the e-Safety co-ordinator who will report it to the headteacher. All incidents will be recorded in the safeguarding log.
- Requests for changes to the filtering will be directed to the e-Safety coordinator in the first instance who will forward these to the head and then the ICT technician.
- All staff are issued with their own username and password for Office 365 access. Trainee teachers and long term supply staff are issued with temporary IDs and the details recorded. Other students/ visitors will be issued with a temporary username/ password on request.
- Pupils use class name logon IDs for their network access.

Mobile / emerging technologies

- Teaching staff at the school are provided with a laptop for educational use and their own professional development. All staff understand that the Acceptable Use Policy applies to this equipment at all times.
- To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network.
- Staff understand that they should use their own mobile phones sensibly and in line with guidance in the Staff Contact and Child Protection policies.
- The Educations and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at her discretion.
- Pictures / videos of staff and pupils should not be taken on personal devices.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community.

E-mail

The school e-mail system is provided and filtered by Office 365 and monitored by AtomIT.

All staff are given a school e-mail address and understand that this must be used for all professional communication.

- Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication.
- Staff are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with the Acceptable Use policy. In addition, they also understand that these messages will be scanned by the monitoring software.
- Everyone in the school community understands that any inappropriate e-mails must be reported to the e-Safety co-ordinator as soon as possible.

Published content

The Head takes responsibility for content published to the school web site but delegates general editorial responsibility to Mrs Scotney (Computing co-ordinator). Staff are responsible for the editorial control of work provided for publication.

- The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.
- The school does not publish any contact details for the pupils.

Digital Media

We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or vide are published or distributed outside the school.

- Photographs published on the website will not identify any individual pupil by name.
- Students' full names will not be published outside the school environment.

Social Networking and online communication

The school currently allows limited access to social networking sites for example, YOU TUBE and email for educational purposes but not for personal use.

Guidance is provided to the school community on how to use online communication safely and appropriately. This includes

- Being selective about publishing personal information.
- Not publishing information relating to the school community.
- How to report issues or inappropriate content.

Unmoderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of such sites as the need arises. Any external matters evolving from a social networking site will not be supported by the school.

Educational Use

School staff model appropriate use of school resources including the internet.

- All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material.
- Where appropriate, links to specific web sites will be provided instead of open searching for information.
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Polices before any activity.

E-safety training

The school has a program of continuing professional development in place that includes; Safeguarding INSET, in school support and E-safety assemblies based on the needs of the staff.

- Educational resources are reviewed by curriculum co-ordinators and disseminated through curriculum meetings / staff meetings / training sessions.
- E-Safety is embedded throughout the school curriculum and visited by each year group as required.
- Pupils in Year 2 are taught how to validate the accuracy of information found on the internet.

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998.

Wider Community

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and password that will be recorded in the school office on request.

Equal Opportunities

Regardless of ability, gender or cultural background, e-safety is an issue which applies to all staff, children and visitors.

Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Child Protection Policy.

- Any suspected illegal activity will be reported directly to the HT or a member of the school's SLT.
- Third party complaints, or complaints from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head or deputy headteacher.
- Breaches of this policy by staff will be investigated by the head teacher. Action will be taken under Croydon's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct.
- Serious breaches of this policy by pupils will be treated as any other serious breach of conduct in line with school Behaviour Policy. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.
- Minor pupil offenses, such as being off-task visiting games or other websites will be handled by the teacher in situ by invoking the school behaviour policy.
- The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate.

This policy was agreed by staff and the Governing Body. This policy was reviewed in Autumn 2017 will be reviewed again in Autumn 2018.