E-Safety Policy

Introduction:

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However the use of these new technologies can put young people at risk within and outside the school.

Timed to coincide with Safer Internet Day 2015, the London Grid for Learning carried out an e-safety survey across London in March 2015. The results have been compiled into one of the UK's richest sources of online safety data, and the final report was published by LGfL and data experts at NFER (National Foundation for Education and Research). - See more at: http://www.lgfl.net/esafety/Pages/E-safety-Survey.aspx#sthash.WuKoTaaf.dpuf

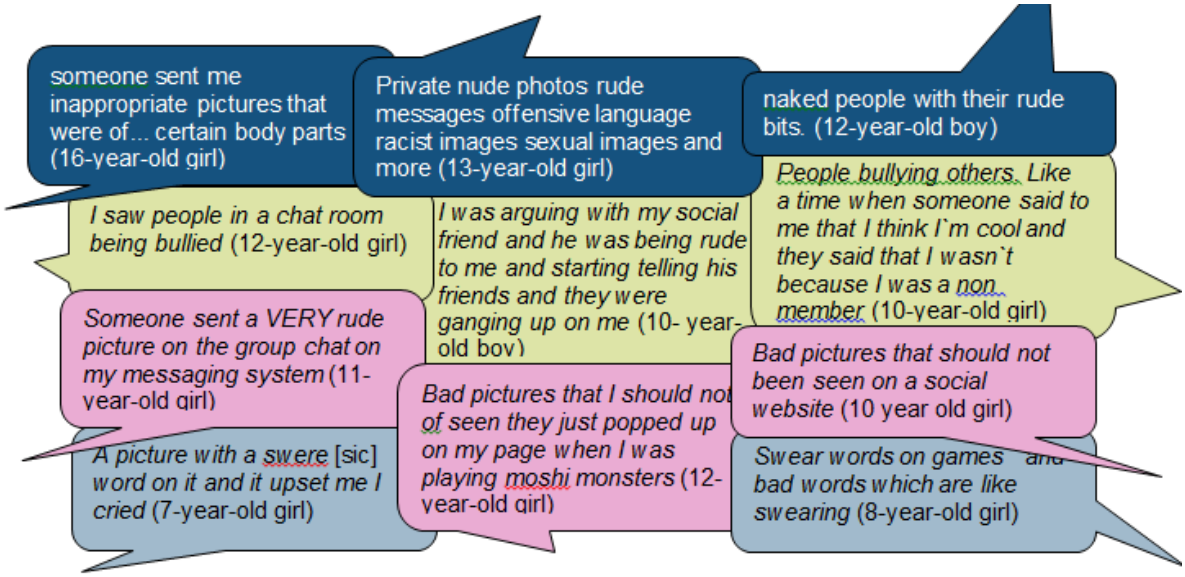
Around one in six young people (16%) reported that they had found or been sent things (pictures, links, videos etc.) online which made them feel uncomfortable or worried.

Of the items reported (n=2,318), one in five (20%) reported seeing rude images including nudity or pornography. A similar proportion (18%) reported personal insults or bullying. 11% reported rude images, and 10% reported offensive language or swear words (multiple response item).

Summary findings

- 9/10 young people access the Internet at home.
- 10/100 of pupils therefore do not
- Just over a third of young people would like more opportunity to use computers at school.
- An increasing number of young people own their own device.
- Very few young people report that they use these devices to access the Internet away from home.
- 40% of 7-year-olds report that their parents always know what they do online; a percentage that (understandably) drops with age.
- Just over 50% of young people use a password on their device at home.
- This is slightly lower for devices that young people use at school. Of those that use a password, half report that someone else knows it, although the majority identified this person as a family member at home. Of those that use a password, a majority reported they do not change it regularly. Over half say that they never change it.
- Young people report that they spend their time online doing school work or studying.
- 3/4 of young people report that they like playing games online but as they get older they play games less and spend more time on social networks and chat sites.

- Many children play games not suitable for their age and a small but concerning minority play 18+ rated games.
- Of the young people playing age inappropriate games, 2/3 are boys.
- Over 50% of young people report that they use social network sites. Of those young people that use social network sites, just over 1/3 have made friends with people online that they did not know before and nearly half of these have gone on to meet this person in real life.Boys are more likely to have made friends with someone they didn't know online and to meet in real life. These meetings were arranged using games consoles, indicating that these relationships were likely to have been made through online games.
- The issue that affects the most children is bullying. 1/5 young people report that they have been bullied online.
- Around 1/6 young people reported that they have found or been sent things online which made them feel uncomfortable or worried. Items frequently reported included rude images (nudity or pornography), personal insults or bullying,offensive language or swear words. Of more concern, but less prominent were the small number of young people (five per cent or less of those that reported that they had found or been sent things online which made them feel uncomfortable or worried) who reported seeing 'rude' videos or seeing people being killed, hurt or war-related material.



The breadth of issues classified within e-safety is considerable, but can be categorised into three areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful material
- **contact:** being subjected to harmful online interaction with other users
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

Some of the dangers young people may face include:

- Access to **illegal, harmful** or **inappropriate** images or other content
- **Unauthorised access** to / loss of / sharing of personal information

- The risk of being **subject to grooming** by those with whom they make contact on the internet.
- The **sharing / distribution of personal images** without an individual's consent or knowledge
- **Inappropriate communication** / contact with others, including strangers
- **Cyber-bullying**
- Access to **unsuitable video / internet games**
- An **inability** to **evaluate** the **quality**, **accuracy** and **relevance** of information on the internet
- **Plagiarism** and copyright infringement
- **Illegal downloading** of music or video files
- The potential for **excessive use** which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good practice to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Development Monitoring & Review of this Policy
Our e-Safety Policy has been written by the school e-safety development group made up of the following staff:

- School e-Safety Co-ordinator (Mohammed Badrul Islam)
- Senior Leaders/DSL (MD Nazmul Haque)
- Student Support Co-ordinator (Muhammad Musharraf Hussain)

Role of Proprietors and Governors
The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Ensure that e-safety education for pupils, staff and parents follows the advice of national organisations and helps to commit all concerned to lifelong e-safety.

- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Principal in regards to training, identified risks and any incidents.
    - Chair the e-Safety Development Group
    - Report any findings to the proprietors

Role of the Principal

Reporting to the governing body, the Principal has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer (or more than one), as indicated below.

The Principal will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Coordinator has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

Whole school consistent approach:

- All teaching and non-teaching staff can recognise and are aware of e-safety issues
- The senior leaders make e-safety a priority across all areas of the school
- E-safety is embedded in the curriculum and taught progressively across key stages
- A high priority is given to training in e-safety: all staff and pupils have been trained; the school has built links with LA schools to extend expertise widely and build internal capacity
- Pupils know how to report an incident
- The contribution of pupils, parents and the wider school community is valued and integrated.

This policy builds on the guidelines and guidance given by local authority (although the school is an independent school), the London Grid for Learning and Ofsted. It has been agreed by the Senior Leadership Team. This e-Safety Policy and its implementation will be monitored by senior staff and will be reviewed annually.

The impact of the policy will be monitored using:

- Incident logs
- Internal monitoring using filtering software
- Feedback from survey and questionnaires issued to students, parents and carers and staff

Scope of this policy:
This policy applies to all members of the school community (including staff, students, parents and carers, visitors, community users) who have access to and are users of the school's ICT systems both in and out of school.

Teaching and learning
The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Students use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?
Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between students world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with Tower Hamlets LA and the DfE

How can Internet use enhance learning?

- The school Internet access will be designed expressly for student use and **will include appropriate filtering.**
- **Students will be taught what Internet use is acceptable and what is not** and given clear objectives for Internet use in lessons.
- Internet access will be planned to enrich and extend learning activities.
- **Staff should guide students in on-line activities** that will support the learning outcomes planned for the students' age and maturity.

- **Students will be educated in the effective use of the Internet in research**, including the skills of knowledge location, retrieval and evaluation.

How will students learn how to evaluate Internet content?

- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and students complies with copyright law.
- **Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy**.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

Managing Information Systems

How will information systems security be maintained?

- Users must take responsibility for their network use.
- Workstations will be secured against user mistakes and deliberate actions.
- Servers are located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be pro-actively managed.

Wide Area Network (WAN) security issues include:

- All Internet connections are arranged using RM as our ISP
- Firewalls and switches are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership basis between school and Staffordshire Learning Technologies.
- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The Network Manager will review system capacity regularly.

How will e-mail be managed?

- Students may only use their school e-mail accounts.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts will be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

How will published content be managed?

- The contact details on the website should be the school address, e-mail and telephone number. Staff or students' personal information must not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Can student's images or work be published?

- Written permission from parents or carers will be obtained before images of students are electronically published.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Work can only be published with the permission of the student and parents.

How should personal data be protected?

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individuals rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Personal data will be recorded, processed, transferred and made available according to the terms of the Data Protection Act 2018 & GDPR.

How should personal data be protected?

The Data Protection Act 2018 and GDPR applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards, which must be satisfied when processing personal data (information that will identify a living individual).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorized processing, access, loss, destruction or damage

How will Internet access be authorised?

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications.
- All staff must read and sign the "Staff Code of Conduct' and 'Acceptable Use Agreement" before using any school ICT resource.
- All pupils must sign the 'Pupil Acceptable Use Agreement' before using and school ICT resource
- All network users have to agree to the school's Acceptable Use Policy (AUP) each time they log on to the network.

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will e-safety complaints be handled?

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Principal.
- Students and parents will be informed of the complaints procedure.
- Parents and students will need to work in partnership with staff to resolve issues.
- Discussions may be held with appropriate outside agencies
- Sanctions which may be applied by the school include:
  -interview/counselling by the tutor;
  - informing parents or carers;

- removal of Internet or computer access for a period
- other sanctions as appropriate to the level of misuse (including the involvement of appropriate external agencies)

How is the Internet used across the community?

The school will liaise with other organisations to establish a common approach to e-safety. The school will be sensitive to Internet related issues experienced by students out of school, e.g. social networking sites, and offer appropriate advice.

How will the policy be communicated to students?

- E-Safety rules will be posted in rooms with Internet access.
- Students will be informed that network and Internet use will be monitored.
- E-safety awareness will be delivered during computing lessons to raise the awareness and importance of safe and responsible internet use. However, e-safety is the joint responsibility of all staff, students and parents working in cooperation with each other.
- E-safety education will be included in the PSHE, Tutor Time & computing programmes covering both school and home use.

How will the policy be discussed with staff?

- All staff will be given the School e-Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.
- All staff will be expected to sign an 'Acceptable Use Policy' at the start of each academic year (or from their start date if applicable).

How will parents' support be enlisted?

- Parents' attention will be drawn to the school's e-Safety Policy in letters, the school newsletters and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed below under e-Safety Contacts and References.

E-Safety Contacts and References:
School e-Safety Coordinator- Mohammed Badrul Islam
Know IT All website: Know IT All website contains a wide range of e-safety resources for secondary school pupils. They have been produced by Child net International to help secondary school teachers and school staffs understand and address a range of e-safety issues within schools. http://www.childnet.com/resources/kia/

Thinkuknow website: Useful information on e-safety issues for staff, students and parents

- www.thinkuknow.co.uk

CEOP -Child Exploitation & Online Protection centre

- http://www.ceop.gov.uk

National Education Network-NEN provides advice on e-security

www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.childnet.com/cyberbullying-guidance
www.pshe-association.org.uk
educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

This policy must be read alongside the Staff Code of Conduct, the Safeguarding policy, the Anti-bullying policy and the Acceptable Use Agreements for staff and pupils.

Date Policy Reviewed: 12th June 2020

Print Name (Chair of Governors): **Moulana Mohammed Abdul Jalil**

Next Review Date: June 2021

Responsibility for review: Principal / Governors.