Rida Boys
High School

E-SAFETY POLICY

Our school is committed to keeping children safe and healthy in its care and the e- safety policy operates always under the umbrella of the **Safeguarding Policy**. The same 'staying safe' outcome outlined in Every Child Matters agenda will apply equally to the 'virtual' or digital/electronic world of communication.

We recognise that the internet plays a vital role in a child's education and can help enrich and extend learning activities, promote pupil achievement and raise educational standards. The use of the internet also supports the work of staff and helps maintain the school's management/admin system.

Aim

The purpose of the e-safety policy is to maximise the educational benefit and fulfil the obligation of providing quality internet access to children as part of their lifelong learning experience, whilst adopting a safe culture and minimising any associated risks. Children shall be educated about the benefits and the risks of using technology and controlling their online experience.

Internet Access

- The use of internet is a part of the statutory curriculum and an essential tool for staff and children;
- The use of internet enhances learning opportunities;
- The internet is used and integrated into the planning to enrich and extend learning activities;
- The internet shall benefit education by allowing access to various educational resources.

Managing Internet Access

- Internet access is designed particularly for pupils' use reflecting the curriculum requirements and includes filtering appropriate to the age of children;
- Children are given clear objectives for Internet use and are taught what Internet use is acceptable and what is not;
- Children are taught how to evaluate Internet content;
- Children are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation;
- Children are taught to cross-check information and validate information before accepting its accuracy;
- Children are taught how to report unpleasant Internet content or if unsuitable sites are discovered.

Internet access security

- The security and capacity of the school information systems is reviewed regularly;
- Virus protection is installed and updated regularly.

Managing E-mail

- Pupils and staff shall only use approved e-mail accounts on the school system;
- Personal e-mail or messaging between staff and pupils shall not take place;
- Staff shall use the school e-mail address if they need to communicate with pupils about their school work;
- Personal details of themselves or others shall not be revealed in e-mail communication, or arrangement to meet anyone without specific permission;
- On occasions an e-mail shall be authorised before sending to an external organisation just as a letter written on school headed note-paper would be;
- The forwarding of chain letters is not permitted.

Managing web site content

- The point of contact on the school web site shall be the school address, e-mail and telephone number;
- Staff or children's personal information is not published;
- The Governing Body have overall editorial responsibility and ensure that content is accurate and appropriate;
- The school's ethos is reflected in our website, ensuring that information is accurate, well presented and personal security is not compromised;
- Care is taken to ensure that all information is considered from a security viewpoint including the use of photographic material;
- Photographs of pupils are not used without the written consent of the pupil's parents/carers;
- Use of site photographs is carefully selected so that any pupils cannot be identified, or their image misused;
- The names of pupils are not used on the website, particularly in association with any photographs;
- The copyright of all material on the website will be held by the school.

Social networking and chat rooms

- The school blocks/filters access to social networking sites *(including My Space, Facebook, and Twitter);*
- Newsgroups are blocked unless a specific use is approved by the Headteacher;
- Pupils are advised never to give out personal details of any kind which may identify them or their location. I.e. Real name, address, mobile or landline phone numbers, school, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for pupils;
- Pupils are taught the importance of personal safety when using social networking sites and chat rooms;
- Pupils are not allowed to access public or unregulated chat rooms;
- Staff shall not exchange social networking addresses or use social networking sites to communicate with pupils;
- Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil is necessary, the agreement of a member of the SMT shall always be sought first and language used shall always be appropriate and professional.

Managing Filtering

- The school works in partnership with parents/carers; the Local Authority, the DCFS and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly;
- Filtering methods are selected by the school in consultation with its IT partner and with the LA to ensure that they are age and curriculum appropriate;
- Regular checks by Senior Staff is undertaken to ensure that the filtering methods selected are appropriate, effective and reasonable;
- If staff or pupils discover unsuitable sites, the URL and content shall be reported to SMT immediately.

Potential risks

Internet and electronic communications technologies derive huge educational benefits but also carry potential risks. Some of the potential risks are highlighted below:

Content

- Children shall be protected from viewing and/or downloading adult material, violence, racist/hate sites, potential grooming and extremist material;
- Children are made aware of the potential long-term effects of any inappropriate content that they upload themselves, such as photographs, too much personal information or nasty comments about others;
- Children are educated about the need to understand that anyone can publish anything they wish on the Internet, so it may be inaccurate;
- In addition, children are educated about the need to understand about inappropriate use of Internet and respecting copyright issues.

Contact

There are people who will try their utmost to gain access to children to do them harm. The dangers of contact with persons unknown are made clear.

Communication

- Children shall be protected and made aware of the potential dangers of digital communication (i.e. you can never be 100% sure that you know who you are communicating with!);
- Safe use/potential dangers of email use, instant messaging, chat rooms, social networking sites etc. are explored and made clear to pupils;
- The dangers of using digital imaging devices such as cameras and webcams to display images should also be highlighted;

Culture

The way that some children use the Internet can lead to depersonalisation (forgetting that in the virtual world, there is a real person) and this can lead to cyber bullying, which can become far more extreme and wide-ranging than ‘face to face’ bullying.

Commerce

Children shall be protected from and educated about issues surrounding commercial marketing such as spam, phishing etc.

Assessing risks

Some material available through the Internet is unsuitable for children. The school takes all reasonable precautions to ensure that users access only appropriate material. However, due to the nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

Access to any websites involving gambling, games or financial scams is strictly forbidden and shall be dealt with accordingly.

Introducing the e-safety policy to children

- Children are informed that Internet use is only with adult supervision;
- Pupils are informed that internet use will be closely monitored, and that misuse will be dealt with appropriately;
- Pupils are instructed in responsible and safe use before being allowed access to the Internet;
- Lesson on e-safety and responsible Internet use, covering both school and home use, are taught.

Staff and the e-Safety policy

- All staff are given the school e-Safety policy and its importance explained;
- Staffs are made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential;
- Staff shall not use personal email or mobile technology to contact students. If contact is necessary school telephone / email account shall be used;
- It is essential that teachers and learning support staff are confident about using the internet in their work and shall be given opportunities to discuss issues and develop appropriate teaching strategies;
- All new staff are given a copy of the policy during their induction.
- Staff development in safe and responsible use of the internet shall be provided as required.

Parent/Carers Support

- Parents/carers are informed of the School's Internet Policy which can be accessed on the school website;
- Parents' attention is drawn to the School e-Safety Policy in newsletters;
- Any issues concerning the internet shall be handled sensitively to inform parents/cares without undue alarm;
- Parents and carers shall from time to time be provided with additional information on E- safety.
- The school requires all new parents to sign the parent/ pupil agreement when they register their child with the school.
- Periodically parent workshops are held to update awareness on

Handling e-safety complaints

- Pupils and parents are informed of the complaints procedure;
- They are informed of how and where to report incidents;
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures;
- Complaints of Internet misuse are dealt with by SMT;

- Any complaint about staff or pupil misuse shall be referred to SMT/GB immediately;
- Parents/carers and pupils work in partnership with the school staff to resolve any issues;
- Sanctions within the school discipline policy include:
  – Interview by member of SMT;
  – Informing parents or carers;
  – Removal of Internet or computer access for a period.

Roles and responsibilities

SMT ensure that:

- All staff and volunteers understand and are made aware of the school's E-Learning/Safety Policy and arrangements;
- Staff understand that misuse of the internet may lead to disciplinary action and possible dismissal;
- All staffs are included in E-Safety training;
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers;
- ICT security is maintained;
- Staff attend appropriate training;
- Support and training for staff and volunteers on E-Safety is provided;
- the school's ICT systems are regularly reviewed with regard to security;
- Virus protection is regularly reviewed and updated;
- Regularly check files on the school's network.

The Governing Body of the school will ensure that:

- There is a senior member of the school's leadership team who is designated to take the lead on E-Learning/Safety within the School;
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures;
- All staff and volunteers have access to appropriate ICT training.