E-Safety Policy

Throughout this policy 'parents' denotes those with parental responsibility.

NOTICE: DURING THE COVID-19 PANDEMIC, PLEASE READ THIS POLICY ALONGSIDE THE REMOTE LEARNING POLICY.

1. Mission Statement

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. We strive to make full use of these technologies to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the centre's management information and administration systems. We believe access to the Internet is an entitlement for pupils who show a responsible and mature approach to its use and that the centre has a duty to provide pupils with quality Internet access. The centre also recognises that pupils will use these technologies outside of the centre and need to learn how to take care of their own safety and security. We fully recognise our responsibilities for e-safety, including a responsibility to educate our pupils about the benefits and risks of using new technology and the provision of safeguards and information for all users to enable them to control their online experiences.

This Policy applies to all members of the centre community (including staff, pupils, volunteers, parents, visitors, community users) who have access to and are users of centre Information and Communication Technology (ICT) systems, both in and out of the centre. All adults, including volunteers, working in or on behalf of the centre share the responsibility to keep children safe from harm

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of a school setting, but is linked to the child's membership of the school. In this respect, we will take all allegations of cyber-bullying or other e-safety incidents very seriously.

The centre/school will deal with such incidents within this Policy and associated Behaviour and Anti-Bullying policies and will, where known, inform parents of incidents of inappropriate e-safety behaviour that take place out of the centre.

1.1 Aims and objectives

Our school/centre aims to ensure that children are effectively safeguarded from potential risk of harm and that the safety and well-being of children is of the highest priority in all aspects of the school/centre's work.

Specifically we aim to:

- Ensure that all stakeholders are aware of and take seriously their responsibility to promote and safeguard the online safety of children;
- Use the Internet and other technologies as tools for teaching and learning within the context of educating children and adults in how to use such technology responsibly, giving clear expectations for appropriate use;
- Ensure staff and children understand the dangers that can arise and the procedures for dealing with e-safety incidents;
- Ensure that school Internet access is appropriate for both pupil and adult use and includes filtering appropriate to the age of pupils;
- Guide pupils in using technologies and developing skills in ways appropriate to their age and maturity.

2. Roles and Responsibilities

2.1 Executive Headteacher and Assistant Headteachers

Are responsible for:

- Ensuring the E-Safety Policy is disseminated and its importance explained;
- Ensuring the safety (including e-safety) of members of the Centre Community;
- Ensuring that relevant staff receive suitable continuing professional development (CPD) to enable them to carry out their e-safety roles and to train other colleagues, as is relevant;
- Having familiarity with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Executive Headtecher and Assistant Headteachers are designated person for child protection and as such should be:

- Trained in e-safety issues;
- Aware of the potential for serious child protection issues to arise from: sharing of personal data; access to illegal/inappropriate materials; inappropriate online contact with adults/strangers; potential or actual incidents of grooming and cyber-bullying.

2.2 Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- They have read, understood and signed the school Staff Acceptable Use Policy Agreement;
- They report any suspected misuse or problem to the Executive Headteacher or Assistant Headteacher;
- Digital communications with pupils (email etc) are only on a professional level and carried out using official centre systems;
- E-safety issues are embedded in all aspects of the Curriculum and other centre activities;
- Pupils understand and follow the school E-Safety and Acceptable Use Policy;
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor ICT activity in lessons, extra-curricular and extended school activities;
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices, monitor their use and implement current school policies with regard to these devices;

- In lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches;
- They safeguard the security of their username and password and do not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security and MUST change their password immediately;
- They report immediately to the Centre Director any infringements in the centre's filtering of which they become aware or any sites that are accessed, which they believe should have been filtered;
- They do not attempt to use any programmes or software that might allow them to bypass the filtering or security systems in place to prevent access to such materials.
- They at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- They use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data.

2.3 Pupils

Pupils are expected to:

- Use the centre ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be required to sign before being given access to school systems;
- Report abuse, misuse or access to inappropriate materials, once they know how to do so;
- Know and understand centre policies and procedures on the use of mobile phones, digital cameras and hand held devices including the taking or use of images;
- Understand that cyber-bullying is a form of bullying and will not be tolerated;
- Safeguard the security of their username and password and not allow other users to access the systems using their log on details. They should report any suspicion or evidence that there has been a breach of security so their password can be changed;
- Understand the importance of adopting good e-safety practice when using digital technologies out of school and recognise that the centre's E-Safety Policy covers their actions out of the centre, if related to their membership of the centre.

2.4 Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents do not fully understand the issues and are less experienced in the use of ICT than their children. The School will therefore take every opportunity to help parents understand these issues through e-safety evenings, newsletters, letters, website and information about national and local e-safety campaigns or literature.

Parents will be responsible for:
- Endorsing (by signature) the Fair and Safe internet usage letter;
- Accessing the school website in accordance with the relevant Centre Acceptable Use Policy.

3. E-Safety Education

The education of pupils in e-safety is an essential part of the centre's e-safety provision. Children need the help and support of the centre to recognise and avoid e-safety risks and build their resilience. E-Safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

E-Safety education is provided in the following ways:

- Pupils are helped to understand the need to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school;
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

- To STOP and THINK before they CLICK;
- To have strategies for dealing with receipt of inappropriate materials;
- To be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system;
- To understand 'Netiquette' behaviour when using an online environment or email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keep personal information private.

(Also see Internet Access, World Wide Web, Use of Digital and Video Images, Use of email, Use of Social Networking).

4. World Wide Web

- Members of staff are aware of the potential for misuse and are responsible for explaining to pupils, the expectation we have of them.
- Pupils will be guided to sites in lessons that have been checked as suitable and processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Pupils will be monitored when using the Internet when they are allowed to freely search, e.g. using search engines. Staff should be vigilant in monitoring the content of the websites the young people visit and they are expected to use age-appropriate search tools.
- If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to the Director/Proprietor.
- The school/centre will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- There will be a 'no blame' environment that encourages pupils to tell a teacher or other responsible adult immediately if they encounter any material that makes them feel uncomfortable.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils are taught:

- To be critically aware of the materials and content they access on-line and to validate the accuracy of information;
- To know how to narrow down or refine a search;
- To be aware that the author of a website or page may have a particular bias or purpose and to develop skills to recognise what that may be;
- To acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- To understand the issues around aspects of the commercial use of the Internet, as age-appropriate. This may include, risks in pop-ups; buying online; online gaming or gambling;
- What to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher.

5. Acceptable Use

Staff and students are asked to sign a Fair and Safe Internet Usage agreement prior to using any school devices.

6. Use of Digital and Video Images

- When using digital images, staff are expected to inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites.
- Members of staff are allowed to take digital or video images to support educational aims when there is parental consent, but must follow centre policies concerning the sharing, distribution and publication of those images. **Such images should only be taken on centre equipment, the personal equipment of staff should not be used for such purposes.**
- Care should be taken when taking digital or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the centre into disrepute.
- Photographs published on the Website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- There are to be no photographs taken of children in the centre without express written permission from the parents for the purpose.
- Pupils' full names will not be used anywhere on the School Website, in association with photographs.

Pupils are taught:

- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos;
- To understand why they must not post pictures or videos of others without their permission;
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.

7. Use of Email

- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on centre headed paper.
- The forwarding of chain letters is not permitted.

Pupils are taught:

- Not to give out their email address unless it is part of a centre managed project or to someone they know and trust and is approved by their teacher or parent;
- That an email is a form of publishing, where the message should be clear, short and concise;
- That any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on centre headed paper;
- That they must not reveal private details of themselves or others in email, such as address, telephone number, etc.;
- To STOP and THINK before they CLICK and not open attachments unless sure the source is safe;
- That they must immediately tell a teacher or other responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
- Not to respond to malicious or threatening messages;
- Not to delete malicious of threatening emails, but to keep them as evidence of bullying;

- Not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them.

8. Use of Social Networking

Pupils are taught:
- Never to give out personal details of any kind which may identify them or their location;
- Not to place personal photos on any social network space;
- To set passwords, deny access to unknown individuals and block unwanted communications;
- To invite known friends only and deny access to others;
- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.

9. Filtering Policy

The filtering of Internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. No filtering system can guarantee 100% protection against access to unsuitable sites, however, we use web filtering to manage the associated risks and to provide preventative measures which are relevant to the situation in this centre.

9.1 Monitoring

As the filtering system cannot guarantee 100% protection, the centre monitors the activities of users on school equipment as indicated in the School E-Safety Policy and the Acceptable Use Policy. Monitoring will take place as follows:

9.2 Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:
- the PA to the Executive Headteacher

10. Password Security

The school/ centre will be responsible for ensuring that the network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access;
- No user is able to access another's files, without permission (or as allowed for monitoring purposes within the school/ centre's policies);
- Access to personal data is securely controlled in line with the School/centre's policy (see section 12 below);
- Logs are maintained of access by users and of their actions while users of the system ;

A safe and secure username/password system is essential if the above is to be established and will apply to all centre equipment.

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access or data loss. This should apply to even the youngest of users, even if class logons are being used.

11. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Sensitive data will be transferred using encryption and secure password protected devices only. Any data must be securely deleted from devices and secure sites, in line with school/ centre policy once it has been transferred.
The school/ centre will monitor its use of portable computer systems, USB sticks or any other removable media, to ensure that any sensitive data cannot be linked to an individual unless the data is encrypted and password protected.

12. Responding to Incidents of Misuse

It is hoped that all members of the centre community will be responsible users of ICT, who understand and follow this Policy. However, there may be times when infringements of the Policy could take place, through careless or irresponsible use or, very rarely, through deliberate misuse.

If a pupil infringes the E-Safety Policy the incident will initially be referred their teacher. After repeated misuse, access to computers and/or the Internet in the centre may be removed for a set time.

If a staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of HR.

If any apparent or actual misuse appears to involve illegal activity i.e.
- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

the incident must be immediately reported to the PA to Executive Headteacher, who will seek advice from the Local Authority and report to the police and Social Services as advised. Evidence should be preserved to assist investigation.

13. Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by the Executive Headteacher.
- Any complaint about staff misuse must be referred to the Executive Headteacher.

- Complaints of a child protection nature must be dealt with in accordance with centre child protection procedures (See Safeguarding and Child Protection Policy)
- Discussions will be held with the Police if procedures is needed for handling potentially illegal issues.

Policy:
Jennifer Wood, Centre Director (Total Tuition)
Created: August 2018
Reviewed: September 2019 (Total Tuition)
Reviewed: March 2021 (Rosewood Independent School)
Reviewed: August 2021
Reviewed: 1st September 2022, Jennifer Abraham