Teach SouthEast E-Safety Policy

Scope of the Policy

This policy applies to all members of the Teach SouthEast community (including staff, students, volunteers, parents / carers, visitors etc.) who have access to and are users of Teach SouthEast and/or school based ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students 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.

Teach SouthEast will work with our partner schools to will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers (via our placement schools) of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the Teach SouthEast partnership:

Key individuals:

Director: Amy Harper
Deputy Director: Alex Berry
Assistant Directors: Sarah Chapman, Rachel Davis
E-safety Co-Ordinator: Rachel Davis
Network Manager: Simon Bell
Administration manager: Claire Brown
Financial Administrator: Janice Woods

Director and Assistant Directors:

• The Director is responsible for ensuring the safety (including e-safety) of members of the Teach SouthEast community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.

• The Director is responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

• The Director and Assistant Directors should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Coordinator:

• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the e-safety policy.

• Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

• Provides training and advice for staff.

• In the event of an e-safety incident, liaises with placement school ICT technical staff & VLE coordinator.

• Receives reports of e-safety incidents, where applicable, and creates a log of incidents to inform future e-safety developments.

• Reports to the Director.

Network Manager & Network Team:

• Ensure that the Teach SouthEast ICT infrastructure is secure and is not open to misuse or malicious attack.

• Ensure that Teach SouthEast meets the e-safety technical requirements outlined in the Local Authority E-Safety Policy and guidance.

• Ensure that users may only access Teach SouthEast networks through a properly enforced password protection policy, in which passwords are regularly changed.

• Keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

• Makes sure that the use of the network, Virtual Learning Environment *(VLE), remote access,* email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction.

Teach SouthEast Trainees:

• Ensure they have an up to date awareness of e-safety matters and of the e-safety policy and practices in their placement school(s).

• Ensure they have read and understood any placement school(s) ICT Resources Use Policies

• Make sure they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation / action / sanction.

• Ensure that digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems.

• Ensure that they are not ‘friends’ with students on social-networking sites and take every reasonable precaution to ensure that students cannot access personal content posted by them online.

• Ensure that e-safety issues are embedded in all aspects of the curriculum and other school activities.
• Ensure that students understand and follow the school e-safety and acceptable use policy.
• 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, tablet computers, cameras and other hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
• Ensure that students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Education of Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the partnership's e-safety provision. Children and young people need the help and support of their teachers' to recognise and avoid e-safety risks and build their resilience.
• Students should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
• Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
• Staff (Teach SouthEast Trainees) should act as good role models in their use of ICT, the internet and mobile devices.
• E-safety should be a focus in all areas of the curriculum and staff (Teach SouthEast Trainees) should reinforce e-safety messages in the use of ICT across the curriculum.
• Where students are allowed to freely search the internet and/or use tablet computers, staff (Teach SouthEast Trainees) should be vigilant in monitoring the content of the websites the young people visit and the applications they are using.
• Students 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.

Education & Training of Staff (Teach SouthEast Trainees)

It is essential that all trainees receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
• E-Safety training will be made available to trainees.
• All trainees should receive e-safety training as part of their induction programme, ensuring that they fully understand the e-safety policy.
• The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Use of digital and video images - Photographic, Video

• Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
• Care should be taken when taking digital / video images that students and colleagues are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
• Students must not take, use, share, publish or distribute images of others without their permission.
• Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
• Students' full names will not be used anywhere on a website, blog, or trainee documentation, particularly in association with photographs.
• Teach SouthEast will seek permission from trainees before sharing any digital/ video images of them.

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.

Staff must ensure that they:

• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
• 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.