Online Safeguarding Policy

First Published: October 2017 **Review Date:** September 2022

Trust Board Approval: September 2019 **Last Updated:** August 2019

This Online Safeguarding Policy is part of the Trust Development Plan and relates to other policies including those for ICT, bullying and for child protection.

Purpose

Online safeguarding encompasses internet technologies and electronic communications such as mobile phones and wireless technology. This policy highlights the need to educate pupils, students and scholars about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

- The Online Safeguarding Policy and its implementation will be reviewed annually.
- Our Online Safeguarding Policy has been written by the Trust, building on the KCC e–Safety Policy and government guidance and has been discussed with all faculties and by the School Councils.
- Our Policy has been agreed by the Senior Leadership Team in each school and reviewed by Trustees.
- Training for staff, pupils, students and scholars will take place to ensure full understanding and compliance with the policy.

1. Teaching and Learning

1.1. Internet use is important

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction. The Trust has a duty to provide pupils, students and scholars with quality Internet access as part of their learning experience.
- Pupils, students and scholars use the Internet widely outside of school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupils, students and scholars achievement, to support the professional work of staff and to enhance the Trust's management functions.

1.2. Internet use enhances learning

- The Trust's Internet access will be designed to enhance and extend education.
- Pupils, students and scholars will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The Trust will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils, students and scholars complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils, students and scholars.
- Pupils, students and scholars will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.3. Pupils, students and scholars will learn how to evaluate Internet content

- Pupils, students and scholars will use age-appropriate tools to research Internet content.
- Pupils, students and scholars will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils, students and scholars will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Pupils, students and scholars will be taught how to report unpleasant Internet content eg using the CEOP Report Abuse icon

2. Monitoring e-safety

2.1. Maintaining information systems security

- The security of the Trust information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Firewalls will be checked and updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti- virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the Trust's network will be regularly checked.
- The ICT function will review system capacity regularly.
- The use of user logins and passwords to access the Trust network will be enforced.

2.2. Managing email

- Pupils, students and scholars may only use approved email accounts for Trust purposes.
- Pupils, students and scholars must immediately tell a designated member of staff if they receive offensive email.
- Pupils, students and scholars must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official Trust provided email accounts to communicate with pupils, students and scholars and parents/carers, as approved by the Senior Leadership Team.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on School or Trust headed paper would be.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts for school purposes.

2.3. Managing published content

- The contact details on websites should be the school and Trust address, email and telephone number. Staff or pupils, students and scholars personal information must not be published.
- Email addresses will be published carefully online, to avoid being harvested for spam (eg by replacing '@' with 'AT'.)
- The School Principals will take overall editorial responsibility for online content published by the Trust and will ensure that content published is accurate and appropriate.
- The School and Trust websites will comply with guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

2.4. Publishing pupils, students and scholars' images or work

- Images or videos that include pupils, students and scholars will be selected carefully and will not provide material that could be reused.
- Pupils, students and scholars' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils, students and scholars are electronically published.
- Pupils, students and scholars' work can only be published with permission from themselve or their parents/carers.
- Written consent will be kept by the school where pupils, students and scholars' images are used for publicity purposes, until the image is no longer in use.
- The Trust will have a policy regarding the use of photographic images of children which outlines policies and procedures.

2.5. Managing social networking, social media and personal publishing

- The Trust will control access to social media and social networking sites.
- Pupils, students and scholars will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, School attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using social media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school websites with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil, student and scholar use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the Trust where possible.
- Pupils, students and scholars will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils, students and scholars will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the Trust community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding pupils, students and scholars' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the Turner Schools Acceptable Use Policy.

2.6. Managing filtering

- The Trust's broadband access will include filtering appropriate to the age and maturity of pupils, students and scholars.
- The Trust will work with KCC and the ICT function to ensure that filtering policy is continually reviewed.
- The Trust will have a clear procedure for reporting breaches of filtering. All members of the Trust community (all staff and all pupils, students and scholars) will be aware of this procedure.

- If staff or pupils, students and scholars discover unsuitable sites, the URL will be reported to the ICT function who will then record the incident and escalate the concern as appropriate.
- The Trust filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the Trust filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and, where appropriate, with consent from the Senior Leadership Team.
- The Senior Leadership Team in each school will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the Trust believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP
- The Trust's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, students and scholars, with advice from the ICT function.

2.7. Managing video communication

- All video communication equipment in the classroom must be switched off when not in use and not set to auto answer.
- External IP addresses will not be made available to other sites.
- Video communication contact information will not be put on school Websites.
- The equipment must be secure and if necessary locked away when not in use.
- Trust video communication equipment will not be taken off school premises without permission.
- Responsibility for the use of the video communication equipment outside School time will be established with care.

Users

- Pupils, students and scholars will ask permission from a teacher before making or answering a video communication.
- Video communication will be supervised appropriately for the pupils, students and scholars' age and ability.
- Parents and carers consent should be obtained prior to children taking part in video communications.
- Only key administrators should be given access to video communication administration areas or remote control pages.
- Unique log on and password details for the educational video communication services should only be issued to members of staff and kept secure.

2.8. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use across the Trust is allowed.
- Pupils, students and scholars will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the Trust Acceptable Use or Mobile Phone Policy.

2.9. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and General Data Protection Regulation.

3. Policy Decisions

3.1. Authorising Internet access

- The Trust will maintain a current record of all staff, pupils, students and scholars who are granted access to the Trust's network.
- All new staff will read and sign the 'Trust Acceptable Use Policy' before using any ICT resources. Existing staff are reminded of the requirement to adhere to all Trust Policies.

- When considering access for vulnerable members of the Trust community (such as with children with special education needs) the Trust will make decisions based on the specific needs and understanding of the pupils, students and scholars (s).
- Secondary students/scholars will apply for Internet access individually by agreeing to comply with the 'Trust e-Safety Rules' and 'Acceptable Use Policy'.

3.2. Risk assessment

- The Trust will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global, changing and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a Trust computer. Neither the Trust nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The Trust 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 1990/1998 and breaches will be reported to Kent Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

3.3. Responding to any incidents of concern

- All members of the Trust community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The ICT function will record all reported incidents and actions taken in the Trust e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The ICT function will inform the Designated Safeguarding Leads of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The Trust will manage online safeguarding incidents in accordance with the Trust discipline/ behaviour policy where appropriate.
- The Trust will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the Trust will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the Trust will contact the Safeguarding Team or e- Safety officer and escalate the concern to the Police
- If the Trust is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.
- If an incident of concern needs to be passed beyond the Trust then the concern will be escalated to the e-Safety officer to communicate to other Schools in Kent.

3.4. E-Safety complaints

- Complaints about Internet misuse will be dealt with under the Trust's complaints procedure.
- Any complaint about staff misuse will be referred to the Principal.
- All e-Safety complaints and incidents will be recorded by the Trust, including any actions taken.
- Pupils, students and scholars and parents/carers will be informed of the complaints procedure.
- Parents/carers and pupils, students and scholars will need to work in partnership with the Trust to resolve issues.
- All members of the Trust community will need to be aware of the importance of confidentiality and the need to follow the official Trust procedures for reporting concerns.
- Discussions will be held with the local Police Safer Academy's Partnership Coordinators and/or Children's Safeguarding Team to establish procedures for handling potentially illegal issues.

- Any issues (including sanctions) will be dealt with according to the Trust's disciplinary, behaviour and child protection procedures.
- All members of the Trust community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the Trust community.

3.5. Internet use across the community

- The Trust will liaise with local organisations to establish a common approach to e-Safety.
- The Trust will be sensitive to Internet-related issues experienced by pupils, students and scholars out of school, e.g. social networking sites, and offer appropriate advice.
- The Trust will provide appropriate levels of supervision for pupils, students and scholars who use the internet and technology whilst on the school site.
- The Trust will provide an Acceptable Use Policy for any guest who needs to access the Trust computer system or internet on site.

<u>Cyberbullying</u>

3.6. How will Cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of the Trust community will not be tolerated. Full details are set out in the Trust's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the Trust community affected by cyberbullying.
- All incidents of cyberbullying reported to the Trust will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, students, scholars, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The Trust will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, students, scholars, staff and parents/carers will be required to work with the Trust to support the approach to cyberbullying and the Trust's online safeguarding ethos.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at the school for the user for a period of time. Other sanctions for pupils, students, scholars and staff may also be used in accordance to the Trust's anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils, students and scholars will be informed.
    - The Police will be contacted if a criminal offence is suspected.

3.7. Managing Learning Platforms (if applicable)

- SLT and staff will regularly monitor the usage of the Learning Platform (LP) by pupils, students and scholars and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils, students, scholars /staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, student, scholar, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

- When staff, pupils, students and scholars etc leave the Trust their account or rights to specific Trust areas will be disabled or transferred to their new establishment.
- Any concerns about content on the LP may be recorded and dealt with in the following ways:
  a) The user will be asked to remove any material deemed to be inappropriate or offensive.
  b) The material will be removed by the site administrator if the user does not comply.
  c) Access to the LP for the user may be suspended.
  d) The user will need to discuss the issues with a member of SLT before reinstatement.
  e) A pupils/student/scholars' parent/carer may be informed.
- A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Pupils, students and scholars may require editorial approval from a member of staff. This may be given to the pupil, student and scholar to fulfil a specific aim and may have a limited time frame.

4. Mobile phones and personal devices

4.1 Use of Mobile Phones

- The use of mobile phones and other personal devices by pupils, students, scholars and staff in Trust will be decided by the Trust and covered in the Acceptable Use Policy.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the Trust community and any breaches will be dealt with as part of the Trust discipline/behaviour policy. In primary schools, pupils, students and scholars will hand their mobile phones into the office at the start of the school day and collect at the end of the day.
- Trust staff may confiscate a phone or device if they believe it is being used to contravene the Trust's behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil, student and scholar or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- The use of personal devices as network hot-spots is strictly forbidden.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The Trust accepts no responsibility for the loss, theft or damage of such items. Nor will the Trust accept responsibility for any adverse health effects caused by any such devices, either potential or actual.

4.2 Pupils, students and scholars' Use of Personal Devices

- Mobile phones should be switched off and at the bottom of the pupils, students and scholars' bag at all times. If a pupil/student/scholar breaches the Trust policy then the phone or device will be confiscated and will be held in a secure place in accordance with the Trust policy.
- Phones and devices must not be taken into examinations. Pupils, students and scholars found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in their withdrawal from either that examination or all examinations.
- If a pupil/student/scholar needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office
- Pupils, students and scholars should protect their phone numbers by only giving them to trusted friends and family members. Pupils, students and scholars will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

4.3 Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a Trust phone where contact with pupils, students and scholars or parents/carers is required.
- Mobile phones and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the Trust policy then disciplinary action may be taken.

5. Communication Policy

5.1. How will the policy be introduced to pupils, students and scholars?

- All users will be informed that network and Internet use will be monitored.
- Pupil, student and scholar instruction regarding responsible and safe use will precede Internet access.
- An e-Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where pupils, students and scholars are considered to be vulnerable.

5.2. How will the policy be discussed with staff?

- To protect all staff and pupils, students and scholars, the Trust will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The Trust will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils, students and scholars.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within Trust. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

5.3. How will parents' support be enlisted?

- Parents' attention will be drawn to the Trust Online Safeguarding Policy in newsletters, the School prospectus and on the school/Trust website.
- A partnership approach to online safeguarding at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e- Safety at other attended events eg parent evenings and sports days.

- Parents will be encouraged to read the Trust Acceptable Use Policy for pupils, students and scholars and discuss its implications with their children.
- Information and guidance for parents on e-Safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

Appendix: e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

e–Safety Officer, Children's Safeguards Team, Families and Social Care, Kent County Council. The e-Safety Officer is Rebecca Avery email: esafetyofficer@kent.gov.uk Tel: 01622 221469

Childline: www.childline.org.uk

Childnet: www.childnet.com

Children's Officer for Training & Development, Children's Safeguards Team, Families and Social Care, Kent County Council.
The Children's Officer for Training & Development is Mike O'Connell email: mike.oconnell@kent.gov.uk Tel: 01622 696677

Children's Safeguards Team: www.kenttrustweb.org.uk?safeguards

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kent e–Safety in Academys Guidance: www.kenttrustweb.org.uk?esafety

Kent Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 01622 690690 or contact your Safer Academys Partnership Officer. Also visit www.kent.police.uk or www.kent.police.uk/internetsafety

Kent Public Service Network (KPSN): www.kpsn.net

Kent Safeguarding Children Board (KSCB): www.kscb.org.uk

Kidsmart: www.kidsmart.org.uk

Academies e–Safety Blog: www.kenttrustweb.org.uk?esafetyblog

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com