TRANSFORM TRUST
'Together we Achieve'

Transform Trust

E-Safety Policy

Introduction

Information Communication and Technology (ICT) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the every day lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our children with the skills to access lifelong learning and employment.

ICT covers a wide range of resources including: web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning platforms and virtual learning environments
- Email and instant messaging
- Chat rooms and social networking
- Blogs and wikis
- Podcasting
- Video broadcasting
- Music downloading
- Gaming
- Mobile/smart phones/tv's with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Transform Trust we understand the responsibility to educate our pupils in E-Safety issues and schools will teach children the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the Internet and related technologies in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile Internet; technologies provided by the school such as PCs, laptops, iPads, whiteboards, digital video equipment etc., and technologies owned by pupils and staff, but brought onto school premises such as laptops, mobile phones, camera phones and portable media players etc.

Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the schools, the Headteachers and Chairs of Governors ultimately have responsibility to ensure that this policy and practices are embedded and monitored. Schools should have a named E-Safety Co-ordinator who may also have

other responsibilities across the school. All members of the school communities should be made aware of who their E-Safety Co-ordinator is. It is the role of the E-Safety Co-ordinator to keep abreast of current issues and guidance through organisations such the local authority, child exploitation and online protection (CEOP) and Childnet.

The Headteacher and/or E-Safety Co-ordinator should update senior leaders and governors to ensure that all senior leaders and governors have an understanding of the issues at their school in relation to local and national guidelines and advice.

Writing and Reviewing the E-Safety Policy

This policy includes a number of Acceptable Use Agreements for:

- staff, governors, visitors and contractors;
- parents/guardians
- pupils – split KS1 and KS2

these are to protect the interests and safety of the whole school community. They are linked to other mandatory and school safeguarding policies such as safeguarding and child protection, behaviour, health & safety and anti-bullying etc.

Our E-Safety Policy has been produced in conjunction with local authority and government guidance. It has been approved by the Executive Team of the Trust and the Trust Board. The E-Safety Policy will be reviewed bi-annually by the Executive Team and the Trust Board.

E-Safety Skills Development for Staff

- Staff have received information and training on E-Safety issues through the E-Safety Co-ordinator in schools.
- Staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff receive information on the school's Acceptable Use Agreement as part of their induction.
- ALL staff are expected to incorporate E-Safety activities and awareness within their lessons where and when appropriate.
- E-Safety rules are brought to the attention of the children on a regular basis and children are aware of what to do if they access inappropriate material.

E-Safety Information for Parents/Carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being used on the school website. The school website contains useful information and links to sites such as Thinkuknow, CEOP and other safeguarding sites.
- Schools send out relevant E-safety information through newsletters and the school website.

Community use of the Internet

- External organisations using any of our school's ICT facilities must adhere to the E-Safety Policy. It is up-to-the school to ensure that a copy of this Policy is provided and/or available.

Teaching and Learning - Internet use will enhance learning

- Schools will provide opportunities within a range of curriculum areas to teach E-Safety.
- Educating pupils on the dangers of technologies may be encountered outside the school is done informally when opportunities arise and as part of the E-Safety curriculum.
- E-Safety posters are displayed in classroom and on school websites.
- Other opportunities as identified by individual schools.

Acceptable Use Policies

All Acceptable Use Policies are given in the attached appendix.

Managing Internet Access – Information System Security

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages. discuss ideas and publish material, which makes it both art invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- Each School will review its IT systems capacity and security regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Trust and other IT providers (if not the Trust provider). Section 26 of the Counter-Terrorism and Security Act 2015 (the Act) places a duty on certain bodies ("specified authorities" listed in Schedule 6 to the Act), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn. into terrorism". Part of our duty relates to ensuring children are safe from terrorist and extremist material when accessing the Internet in schools by establishing appropriate levels of filtering.

Published content and the school website

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. It is up to School Leaders to ensure that the school's website is accurate and appropriate.

Publishing pupils' images and work

- Written permission from parents/carers will be obtained before photographs/videos of pupils are published on school websites. Consent forms are considered valid for the entire period that the child attends school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully so that individual pupils cannot be clearly identified.

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

Social Network and Personal Publishing

- Schools will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them, school will advise them never to give out personal details of any kind, which may identify them or their location
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils will be asked to report any incidents of bullying to the school.
- It is illegal for children under the age of 13 to have social media accounts.
- We would encourage all staff to use their discretion when using social media sites and accepting friends requests from the school community. We would expect all staff to report to the Headteacher any malicious social media postings regarding the school or staff members.

Managing Filtering

- Schools will work with their Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If pupils or staff discover an unsuitable site, it must be reported to the E-safety co-ordinator in schools.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Emerging Technologies

- Schools will assess emerging technologies for educational benefit and a risk assessment will be carried out by the school before it is used.
- Schools will monitor the use of portable media such as memory sticks as potential sources of computer virus and inappropriate material.
- Schools will have their own procedures for pupils who bring personal mobile devices/phones to school.
- The sending of abusive or inappropriate. text messages outside school is forbidden, this includes material of a sexual nature e.g. "sexting".
- Staff will use a school phone where contact with pupils is required.
- Staff should not use personal mobile phones during designated teaching sessions.

Protecting Personal Data

The school will hold personal information on its systems for as long as a member of staff remains a member of the school community and remove it in the event of that member of staff leaving, or until it is no longer required for the legitimate function of the school. The school will ensure that all personal

information supplied is held securely, in accordance with their policies and practices and as defined by the Data Protection Act 1998.

Staff have the right to view the personal information that the school holds about them and to have any inaccuracies corrected.

Policy Decisions - Authorising Internet Access

Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's E-safety rules.

These E-Safety rules will also be displayed clearly in all networked rooms:

- Access to the Internet will be by directly supervised access to specific, approved on-line materials.
- ALL parents/carers will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's E-safety rules and within the constraints detailed in this policy.
- ALL staff (and other adults such as Governors, Contractors, Visitors where appropriate) must read and agree to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security

- Schools will ensure that pupils and staff are issued with usernames and passwords in line with their school practice.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network and MIS systems.

Assessing Risks

All schools will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the Trust can accept liability for the material accessed, or any consequences of Internet access. The school will audit IT provision to establish if the E-safety procedures are adequate and that its implementation is effective.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a Senior Leader in school and reported to the E-Safety Coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety Co-ordinator and, where considered a real cause for concern, reported to the Headteacher (and where necessary the Safeguarding Governor and the Trust's Safeguarding Lead) who will decide an appropriate course of action.

- Any complaint about staff misuse must be referred to the Headteacher (and where necessary the Safeguarding Governor and the Trust's Safeguarding Lead) who will decide an appropriate course of action.
- Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures.
- All schools must publish their Complaints policy online.

Staff and the E-Safety Policy

- All staff will be given a copy of this policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Any ICT device issued to staff remains the property of the school. Users of such equipment should therefore adhere to this policy.

Monitoring and Review

This policy is implemented by schools on a day-to-day basis by all school staff and is monitored by the E-Safety Co-ordinator.