The White Hills Park Trust

A Culture of Excellence

E-Safety Policy

Version control

Scope:	**Applicable to all Trust Schools**
Review date:	**Autumn Term 2023**
Statutory or non-statutory:	**Statutory**
Author/Reviewer:	**Trust IT Services Manager** **October 2020**

Working and learning online has become essential part of our work in schools. We recognise and celebrate the role of the Internet in enhancing our work and contributing to pupil outcomes. However, it is clear that there are dangers, and it is the duty of the Trust and its schools to do everything possible to eliminate or mitigate these dangers.

E-Safety Policy

1. Policy Document

1.1 This policy applies to all members of the Trust community (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of the Trust's ICT systems, both in and out of our academies.

1.2 Our Headteachers are empowered, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and staff are empowered to impose disciplinary penalties for inappropriate behaviour.

1.3 This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of our Trust and schools, but is still linked to membership of the Trust. The Trust will deal with such incidents within this policy and associated behaviour and inappropriate e-safety behaviour that take place out of school. Parents/carers may be informed of concerns via telephone or letter.

2. Roles and Responsibilities

2.1 The following section outlines the roles and responsibilities for the e-safety of individuals and groups within the Trust:

2.2 Trust Board

Trust Directors are responsible for the approval of the e-safety Policy and for reviewing the effectiveness of the policy.

2.3 Headteachers and Senior Leaders

- Headteachers are responsible for ensuring the safety (including e-safety) of members of their school communities.
- Headteachers and senior leaders are responsible for ensuring that relevant staff receive suitable training and development to enable them carry out their e-safety roles and to train other colleagues, as relevant.
- Headteachers and senior leaders will ensure that there is a system in place to
- Each school's senior leadership team (SLT) will receive information regarding any e-safety incidents which will be logged and reviewed by SLT.
- Headteachers and members of each School SLT 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.

2.3 Member of SLT with responsibility for e-safety

- Take day to day responsibility for e-safety issues and oversee the sanctions for breaches of rules relating to e-safety.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide training and advice to staff.
- Liaise with the Local Authority Designated Officer (LADO) or Police as appropriate.
- Liaise with the Trust's ICT technical staff.
- Receive reports of e-safety incidents as part of behaviour monitoring.
- Provide information to the Trust's Executive Team/Board as appropriate.
- Keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection), Childnet, UK Safer Internet Centre and Prevent Radicalisation.

2.5 Trust IT Services Manager/ICT Technical Staff

- Ensure that all reasonable endeavours to ensure the Academy and Trust ICT infrastructure is secure and is not open to misuse or malicious attack and that all aspects of the Trust's ICT systems are secure, in line with the Trust's guidance and policies.

2.6 Teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of current Trust e-safety policy and practices.
- They have read and understood the appropriate ICT agreements.
- They report any suspected misuse or problem to a member of SLT.
- Digital communications with pupils are only on a professional level and carried out using official Trust systems.
- It is understood that social media may play an important part in communication between the school and pupils, parents/carers; however, there is also a need to ensure it is used in an appropriate and safe way. Before any member of staff sets up a resource such as a student blog space, they must seek permission from the Headteacher, and they should ensure that appropriate steps are taken to make such social media 'private' so that only people they approve can access it. The member of staff will then be responsible for the posts made on the site and for moderating the content from other users/contributors.
- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the Trust's 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 Academy activities.

- They are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current best practice with regard to these devices.
- In lessons where internet use is pre-planned, students should be guided to sites that are checked as suitable for their use.

2.7 Designated Safeguarding Lead (and Deputy)

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

2.8 Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The Trust will therefore take every opportunity to help parents understand these issues through school communications and their websites.

Parents and carers will be responsible for:

- Endorsing the Trust policy.
- Accessing the Academy website in accordance with the relevant Acceptable Use Policy.

3. Education and Training

3.1 E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of the ICT programme.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and within the PSHE curriculum. Pupils are taught about British Values and radicalisation.
- Pupils will be taught whenever an opportunity occurs to be critically aware of the material/content they access on-line and be guided to validate the accuracy of information.
- Pupils will be encouraged to adopt safe and responsible use of ICT, the internet, and mobile devices both within and outside school.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff will act as good role models in their use of ICT, the internet and mobile devices.

3.2 Education and Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- E-safety training for all staff via online training and various other mediums.
- All new staff will receive e-safety training as part of their induction programme, ensuring they understand the E-safety Policy and Acceptable Use Policy.

3.3 Training – Governors

Safeguarding training for governors covers the relevant elements of e-safety training. Governors are required to undertake the school safeguarding training on their appointment, and at least annually.

4. Infrastructure, equipment, filtering and monitoring

The Trust will be responsible for ensuring that the academies infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The expectation of user behaviour whilst using these systems is outlined in the relevant IT polices for staff and pupils.

5. Curriculum

E-safety should be a focus in all areas of the curriculum, appropriate to the age and stage of development of pupils. Staff should reinforce e-safety messages in the use of ICT across the curriculum.

- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils 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.
- Pupils should be taught to acknowledge the source of information used when appropriate and to respect copyright when using material accessed on the internet.

6. Use of digital and video images - Photographic, Video

6.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

6.2 The Trust / schools will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students 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.
- Staff are allowed to take digital / video images to support educational aims, but must follow school and Trust policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school/Trust equipment; the personal equipment of staff should not be used for such purposes. They should also only be stored on the Trust's network and not on any personal device.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Trust into disrepute.
- Pupils 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.
- Written or digital consent from parents or carers will be obtained before photographs of students are published on the school / Trust website.
- Be aware that downloading, copying, or printing images from the internet may breach copyright laws.

7. GDPR (General Data Protection Regulation)

Personal data (as defined by the GDPR) will be recorded, processed, transferred, and made available according to GDPR. Please see the relevant GDPR policy for further information.

8. Communications

8.1 A wide range of rapidly developing communications technologies has the potential to enhance learning.

- Users need to be aware that email communications may be monitored.
- Users must immediately report to a member of SLT, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, text, MCAS etc.) must be professional in tone and content. These communications may only take place on official (monitored) Trust systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material'.
- Personal information should not be posted on school / Trust websites. Only names and official email addresses should be used to identify members of staff.

8. Unsuitable / inappropriate activities

9.1 Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously be banned from the Trust and all other ICT systems. Other activities e.g. Cyber-bullying, use of electronic communications to radicalise children or others, is banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities, please be mindful of these. If in doubt, please seek advice from your Headteacher, or the Trust IT Team.

10. The Prevent Duty

10.1 The statutory guidance makes clear the need for schools to ensure that children are safe from radicalisation and extremist material when accessing the internet in schools. The Trust will ensure that suitable filtering is in place, however even the best filtering solutions do not prevent access to every risk. As with other online risks of harm, every member of staff needs to be aware of the risks posed by the online activity of extremist and radicalisation groups.

11. Responding to incidents of misuse

11.1 It is hoped that all members of the Trust 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 or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

11.2 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.
- Radicalisation of others.

The Headteacher must be informed immediately (or Trust COO and CEO, if necessary). The Headteacher and any other relevant members of the SLT must inform the relevant authorities immediately of any concerns/ infringements. The steps taken must all be reported to the Executive Team.