Horizons Specialist Academy Trust

E-Safety Policy

Reviewed by Finance & General Purposes Committee: 14 June 2022

Date of Review: Summer 2023

Responsible officer: IT Manager

Statement of intent

At Horizons Specialist Academy Trust (HSAT), we take our responsibility towards the safety of staff, visitors and pupils very seriously.

The purpose of this policy is to manage and mitigate risks to the ICT systems and users at Horizons Specialist Academy Trust (HSAT). It ensures that;

- We comply with the UK GDPR
- We secure the ICT systems in line with latest government and police guidance.
- We reassure those users of the ICT system that we secure and protect them.

Horizons Specialist Academy Trust has carefully considered and analysed the impact of this policy on equality and the possible implications for pupils, parents and staff with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

Introduction

In today's society, children, young people and adults interact with technologies such as smart phones, games consoles, tablets and the internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of information, ideas, social interaction and learning opportunities involved are greatly beneficial to all, but occasionally place children, young people and adults in danger.

The e-safety policy covers issues relating to children and young people as well as adults and their safe use of the internet, mobile phones, smart watches and other electronic communications technologies, both in and out of school. It includes education for all members of the Trust community on risks and responsibilities and is part of the "duty of care" which applies to everyone working with children and young people.

The e-safety policy is supported by the Trust's Acceptable Use Agreement for staff, Trustees, visitors, pupils and students and the Trust's Child Protection Policy.

The Chief Executive and Board of Trustees have a legal responsibility to safeguard children and young people and this includes online activity.

Teaching and Learning

A number of studies that have been carried out have identified the educational benefits to be gained through the appropriate use of the internet; e-safety is an integral part of this. We believe it is essential for e-safety guidance to be given to the pupils and students on a regular and meaningful basis. E-safety is embedded within the curriculum and we continually look for new opportunities to promote e-safety across the curriculum for example:

- Access to worldwide educational resources including museums and art galleries.
- Inclusion in the National Education Network which connects all UK schools.
- Educational and cultural visits both at home and abroad.
- Vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils, students and staff.
- Professional development for staff with access to national developments, educational materials and effective curriculum practise.
- Access to learning wherever and whenever convenient.

Within the Trust community internet use is part of the curriculum and is a necessary tool for learning and the Trust has a duty to provide pupils and students with quality internet access as part of their learning experience. Internet use is an entitlement for all pupils and students who use the internet widely outside school and need to learn how to evaluate information they receive and take care of their own safety and security.

It is a necessary part of the Trust's teaching and learning to support children and young people to evaluate the quality of information they receive via the media in all forms and develop critical skills. Specifically, information received via the internet, email or text message requires even better information handling and digital literacy skills not least because it may be difficult to determine origin, intent and accuracy therefore a whole curriculum approach is required.

- Pupils and students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils and students will use age appropriate tools to research internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-Trust requirement across the curriculum.
- Pupils and students will be made aware of the impact of Cyber bullying and know how to seek help if they are affected by any form of inline bullying.
- Pupils and students will be made aware of where to seek advice and/or help if they experience problems when using the internet.
- Pupils and students will be made aware of the use of the CEOP button and how to get in touch with organisations such as ChildLine.

Managing Information Systems

It is important to regularly review the security of the whole ICT and Communication system adopted across the Trust. Therefore the following procedures will be followed:

- Virus protection will be updated regularly.
- The security of the Trust information systems and users will be reviewed regularly.
- The transfer of any work related data to any personal device is banned
- The Network Manager will review system capacity regularly.

- Passwords to access the Trust network must be changed regularly and meet the designated complexity rules.

Emails

Emails are an essential means of communication for both staff, pupils and students. Directed email use can bring significant educational benefits. However it is essential that systems are in place to ensure we are safeguarded against spam, phishing and virus attachments as well as data protection.

The following applies to the Trust:

- Pupils and students may only use approved email accounts for school purposes.
- Pupils and students must immediately tell a designated member of staff if they receive an offensive email.
- Pupils and students must not reveal personal information about themselves or others (including staff) in email communication.
- If staff need to communicate with pupils, students or parents and carers they will only do so via use of official Trust provided email accounts.
- The forwarding of chain messages is not permitted.
- Staff will password protect all personal data attached to external email and provide the password in another email.

Management of Published Content

The Trust has a website which can be used to celebrate pupil's and student's work, promote the academies within the Trust and publish resources and reports to keep all key stakeholders informed of all that we do and the following procedures apply:

- Staff, pupils and students personal details will not be published on the website.
- Principals and the CEO will take overall editorial responsibility for online content published by the Trust and will ensure that content published is accurate and appropriate.
- The website will comply with the Trust's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

The use of digital images of children and young people and will be handled with due care and diligence.

- Pupils and students full names will never be published.
- Pupils and students in the care of the Local Authority will never have their images published for public information.
- Written consent will be sought by pupils and students, and parents and carers on admission and can be withdrawn at any time.

Social Networking, Social Media and personal publishing

The internet has constantly evolving online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

Pupils and students will be encouraged through the curriculum to think about the ease of uploading personal information, the associated dangers and the difficulty in removing an inappropriate image or information once published.

Similarly through Professional Learning all staff will be made aware of the potential risks in using social networking sites of personal publishing either professionally with pupils and students or personally. They will also be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

- **Staff are not allowed to be "friends" with any children, young people or families they work with on social networking sites.** (see HSAT Social Networking Guidance) The Trust will control access to social media and social networking sites.
- Pupils and students will be advised never to give out personal information which may identify them or their location.
- All social media and associated tools are currently banned however if staff wish to use social media tools with pupils and students as part of the curriculum they will need to risk asses the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Permission will then need to be sought from the Principal of the Academy and a request made to the ICT Network Manager to allow access to a particular site.
- Pupils and students 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.
- 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.
- Concerns regarding pupil and students use of social networking, media and personal publishing sites (in and out of school) will be raised with their parents or carers, particularly with the use of 18+ 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 school's Acceptable Use Agreement.

Filtering

Access controls commonly described as filtering are managed by the Trust's ICT Team. The Smoothwall Filtering Solution employs a category based filtering system which will for example block gaming unless it is educational. There is dynamic

filtering on all email accounts, Office 365 has multiple layers of spam and virus protection, NOD also integrates with outlook for attachments scanning. If members of the Trust community happen upon an inappropriate site or receive an email with malicious content that has managed to get through the filtering system then it must be reported to the ICT team immediately.

Managing Internet Access

The Trust will allocate internet access to staff, pupils and students on the basis of educational need. In general terms all staff, pupils and students will have access to the internet unless there are circumstances which may require a suspension of access or access under restricted supervision.

- All staff will read and sign the Acceptable Use Agreement. .
- Parents and carers will be asked to read the Acceptable Use Agreement for Pupils and Students and discuss it with their child or young person where appropriate.
- All visitors to any of the academies who require access to the Trust's network or internet will be asked to read and sign the Acceptable Use Agreement.

Managing Incidents of Concern

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However it is important to consider risks associated with the way these technologies can be used. The Trust seeks to develop the skills that children and young people need when communicating and using technologies enabling them to keep safe and secure and act with respect for others. Incidents of concern may include unconsidered jokes and comments, inappropriate actions and illegal activity, the Trust will take the following steps to minimise risk:

- All staff will be made aware of internet breaches by children and young people.
- Appropriate sanctions will be imposed and staff informed of this.
- The Designated Safeguarding lead on each site will be informed of any e-safety breaches involving Child Protection concerns, which will then be escalated appropriately.
- Parents and carers will be informed of any incidents of concern as and when necessary and appropriate to do so.

Managing E-Safety Complaints

Parents, carers, children and young people and staff should all be aware of the Trust's complaints procedure therefore complaints about internet misuse will be dealt with under the complaints procedure. Any complaint about staff misuse will be reported to the E-safety Co-ordinator or Chief Executive.

- Parents, carers, pupils and students will need to work in partnership with the Trust to resolve issues.
- Any issues will be dealt with according to the Trust's behaviour policy and Child protection procedures.

Managing Cyber bullying

When children and young people are the target of bullying via mobile phones, smart watches, gaming or the internet they can often feel very alone, particularly if the adults around then, do not understand cyber bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful, humiliating and a source of anxiety. It is essential that the whole Trust community, parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond to combat the issue.

While bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence.
If the Trust believes that an offence has been committed the Safeguarding and EHA Support Officer will seek advice from CEOP or the local Police.

Other Trust procedures are set out in the Trust's Anti-Bullying Guidance.

PREVENT: The Issue of Radicalisation

The Counter-Terrorism and Security Act 2015, places a legal responsibility on Academies and Trusts to take every effort to protect members of their community from the threat of political radicalisation. The Trust understands its legal responsibility to take every effort to prevent individuals from being drawn into terrorism through the internet or by other means, and to challenge extremist ideas propagated by terrorist organisations.

The Trust approaches this issue in four ways:

Providing a safe online environment
The Trust has strong filters in place to block pupil access to violent or otherwise inappropriate materials. Pupils and students are required to sign up to an Acceptable Use agreement that specifically prohibits them from seeking to access such sites. Internet usage is monitored and disciplinary responses may follow if a pupil's usage breaches our rules or raises concerns. The Trust will also seek to block specific sites and search terms too if they appear to pose a risk to our pupils and students. Furthermore, pupils and students receive advice and instruction from teaching and pastoral staff on safe internet usage.

Assessment of Pupil and Student Behaviours
The pastoral monitoring by staff within the Trust has a vital role to play in preventing radicalisation of pupils and students. All pupils and students are monitored closely

by teachers and support staff with any issues of concern discussed with staff responsible for Safeguarding. Where necessary an intervention or even counselling may be provided. The Trust will also seek advice and support from the local authority and/or the police when concerns regarding pupil or student radicalisation arise.

Staff Training and Information

The Trust recognises that it has a responsibility to provide training to staff on the issue of radicalisation to ensure that they remain vigilant and informed on the issue. It will also ensure staff are aware of how to respond appropriately if concerned about the possible radicalisation of a pupil or student.

Promoting Fundamental Values

The Trust will vigorously promote fundamental British values such as fairness, democracy, tolerance and the rule of law through its PSHE lessons, tutor times, curriculum and all other daily interactions between pupils, students and staff.

Contacts and Resources

Government advice to Trusts on this issue can be accessed here: https://www.gov.uk/government/publications/preventing-extremism-in-schools-andchildrens-services

The Government also provides contact details for alerting authorities to suspected terrorist activity. These include the DfE dedicated telephone helpline and mailbox for non-emergency advice for staff and governors: 020 7340 7264 and counterextremism@education.gsi.gov.uk in addition to the local police and 101.

Sexting in schools and colleges: Responding to incidents and safeguarding young people

This is advice that covers the sharing of sexual imagery by young people. Creating and sharing sexual photographs and videos of anyone under 18 is illegal. Many professionals consider sexting to be the sending and posting of sexual suggestive images, including nude or semi-nude photographs, via mobiles or over the internet. Young people however are more likely to interpret it as writing and sharing explicit messages with people they know. Parents and carers may think of it as flirty or sexual text messages rather than images. It is therefore important that we educate not only children and young people, but adults across the Trust and parents and carers.

Although the production of such imagery described above is likely to take place outside of an academy, the issues that follow on from this are likely to manifest themselves in our academies therefore we need to be able to respond swiftly and confidently to ensure that children and young people are safeguarded, supported and educated.

The guidance aims to support academies in developing procedures to respond to incidents involving youth produced sexual imagery. It also signposts to resources and support.

The procedures outlined in the guidance should be part of the Trusts Child Protection arrangements and all incidents of youth produced sexual imagery should be dealt with as safeguarding concerns.

Sexual harassment, online sexual abuse, sexual violence

Sexual violence and sexual harassment can occur between two children of any age and sex from primary through to secondary stage and into colleges. It can occur through a group of children sexually assaulting or sexually harassing a single child or group of children. Sexual violence and sexual harassment exist on a continuum and may overlap; they can occur online and face to face (both physically and verbally) and are never acceptable. As set out in Part one of Keeping children safe in education (KCSIE), all staff working with children are advised to maintain an attitude of 'it could happen here'. Any incidents of online sexual abuse will be dealt with in accordance to the Trust's Child Protection Policy and Part 5 of Keeping Children Safe in Education.

Resources and support

- In addition to the Local Safeguarding Partner resources, additional advice can be sought via https://www.gov.uk/government/publications/sexting-in-schools-and-colleges.

The following resources can be used to support parents and carers and children and young people with youth produced sexual imagery:

Helplines and reporting

- Children and young people can talk to a ChildLine counsellor 24 hours a day about anything that is worrying them by ringing 0800 11 11 or in an online chat at http://www.childline.org.uk/Talk/Chat/Pages/OnlineChat.aspx
- If parents or carers are concerned that their child or young person is being contacted by adults as a result of having shared sexual imagery they should report to NCA-CEOP at www.ceop.police.uk/safety-centre
- ChildLine and the Internet Watch Foundation have partnered to help children and young people get sexual or naked images removed from the internet. More information is available at http://www.childline.org.uk/explore/onlinesafety/pages/sexting.aspx
- If parents and carers are concerned about their child or young person, they can contact the NSPCC Helpline by ringing 0808 800 5000, by emailing help@nspcc.org.uk, or by texting 88858. They can also ring the Online Safety Helpline by ringing 0808 800 5002.

Advice and information for parents and carers

- The NSPCC has information and advice about sexting available on its website: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/1
- NCA-CEOP has produced a film resource for parents and carers to help them prevent their children coming to harm through sharing sexual imagery: https://www.thinkuknow.co.uk/parents/articles/Nude-selfies-a-parentsguide/.

- Childnet have information and advice about sexting available on its website: http://www.childnet.com/parentsand-carers/hot-topics/sexting

Managing the use of Mobile Phones, Smart Watches and other devices

Mobile phones and smart watches are considered to be an everyday item in today's society. They can be used in a variety of ways to communicate through texting, photography and internet accesses.

However, mobile phones and smart watches can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged.
- Their use can render pupils, students or staff subject to cyberbullying.
- Internet access on phones and personal devices can allow pupils to bypass security settings and filtering.
- They can undermine classroom discipline as they can be used on silent mode.
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils, students or staff.

It is therefore the Trust's policy to advise that all children and young people under 16 leave their mobile phones and smart watches at home and the students who attend the 6th Form at Abbey Hill Academy and them in at reception at the beginning of the day. Failure to comply with this rule will be dealt with through the Trust's behaviour policy.

- The sending of abusive or inappropriate messages or content via mobile phones and smart watches is forbidden by any member of the Trust community and any breaches will be dealt with via the Trust's Behaviour Policy.
- Staff's use of mobile phones and smart watches will not be permitted during any lesson with children and young people.
- Staff are not permitted to contact children, young people and families with their own personal mobile phone or smart watch.
- Staff should not use personal mobile phones to take pictures or videos of pupils, if it is believed that this is the case disciplinary action may be taken.