**E-Safety POLICY**

1. **Introduction**

As the use of digital technology, the internet and social media increases in school and within society, it is part of the Trust’s safeguarding obligations to ensure that our students, staff and parents understand how to remain safe online and whilst using such technology.

1. **Purpose and Scope of this Policy**

2.1 The purpose of this policy is to ensure that the Trust community, which includes the students, staff, parents, volunteers, Governors and visitors, who have access to the Trust’s ICT systems understand how to stay safe whilst using such systems.

2.2 This policy also sets out information regarding student appropriate use of the ICT systems, internet and social media and provides information about how school will monitor and address any behavioural concerns, or incidents of cyberbullying, associated with such use.

2.3 The scope of this policy extends to empower the Senior Leadership Team, where it is reasonable, to regulate the behaviour of students when they are off site and staff can impose disciplinary measures for any incidents of cyberbullying or other inappropriate behavior.

2.4 Any cyberbullying or behavioural incidents associated with this policy will be dealt with in accordance with the Trust Behaviour Policy.

2.3 This policy is applicable to all students, parents, Governors and staff employed by the Trust including permanent, temporary, contracted and supply staff, as well as all volunteers.

1. **Relationship with other policies**

3.1 This policy should be read in conjunction with the following policies:

* Staff Acceptable Use Policy
* Data Protection Policy
* Safeguarding Policy
* Behaviour Policy

1. **Roles and Responsibilities**

Governors/Trustees:

4.1 The Board of [Governors/Trustees] are responsible for the approval of the E- safety Policy and ensuring the effectiveness of the policy.

SLT:

4.2 The Senior Leadership Team are responsible for ensuring the safety (including the e-safety) of the whole Trust community.

4.3 SLT are responsible for ensuring that relevant staff receive suitable training and development to enable them to carry out their e-safety roles and to train other colleagues, as necessary.

4.4 SLT should appoint and provide appropriate training for a member of staff to carry out the E-Safety Officer’s role. This can be a member of the SLT.

4.5 SLT must ensure that there is a system in place to allow for the monitoring and support of the member of staff who carry out the internal E-Safety Officer’s role.

4.6 The SLT will receive information from the E-Safety Officer regarding any e-safety incidents and it is the ultimate responsibility of the SLT to ensure that such incidents are documented and dealt with appropriately. What is deemed appropriate will depend on the nature of the incident.

4.7 The Head/Principal and the 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.

E-Safety Officer:

The E-Safety Officer will:

4.8 take day-to-day responsibility for e-safety issues and oversee any sanctions imposed for breaches of the rules relating to e-safety. For this reason, it is likely (although not essential) that a member of the SLT carry out this role.

4.9 be responsible for ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.

4.10 provide training and advice to all staff.

4.11 liaise with the DSL (if this role is held by a different member of staff) and the Local Authority Designated Officer (LADO) or the police as appropriate.

4.12 Liaise with the ICT technical staff where appropriate.

4.13 Receive reports regarding e-safety incidents as part of behaviour monitoring.

4.14 Provide information to SLT and the Governors/Trustees on e-safety incidents, practices and measures, where appropriate.

4.15 Keep abreast with current issues, policies and guidance regarding e-safety through organisations such as CEOP (Child Exploitation and Online Protection), Childnet, UK Safer Internet Centre and Prevent.

ICT Technical Staff

4.16 It is the responsibility of the ICT Technical staff to ensure that the trust ICT infrastructure is secure and is not open to misuse or malicious attack and that all aspects of the ICT systems are secure in line with the relevant policies and procedures.

4.17 It is the responsibility of the ICT Technical staff to liaise with the E-safety Officer with any information that is relevant to the role of the E-Safety Officer, including if they become aware of any misuse of the ICT systems.

Designated Safeguarding Lead

4.18 The DSL should be trained in e-safety issues and be aware of the potential for serious child protection issues arising from the use of digital technology. Such risks include:

* Access to illegal or inappropriate materials/content,
* Inappropriate online contact with strangers,
* Potential or actual issues of grooming,
* Cyber-Bullying

The Keeping Children Safe in Education Policy should be followed in the case of any such incidents.

All staff:

4.19 All staff have a responsibility to ensure that they follow this policy to keep themselves and the students safe online and when using digital technology.

4.20 All staff should ensure that they have an up-to-date awareness of e-safety matters and carry out any relevant training as directed by the E-Safety Officer and/or a member of SLT.

4.21 All staff must read and follow the relevant Acceptable Use Policy and sign to state that they agree to the terms of that policy.

4.22 All staff must report any e-safety incidents to the E-Safety Officer and, where necessary, the DSL.

4.23 It is understood that social media can play an important part in communication between the trust and the students, parents/carers and wider community. It is necessary to ensure that social media 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 Head/Principal and they should ensure that appropriate steps are taken to make sure such social media is ‘private and secure.’ The member of staff would then be responsible for any posts made on that site and for moderating the content from other users.

4.24 All staff understand and ensure that e-safety issues are embedded in all aspects of the curriculum.

4.25 All staff are responsible for ensuring that students understand and follow this E- Safety Policy and any additional Pupil Acceptable Use Policy.

4.26 All staff are responsible for educating pupils on appropriate research skills and the need to avoid plagiarism and uphold copyright regulations.

4.27 All staff are responsible for monitoring the use of ICT devices in their lessons.

4.28 All staff are responsible for ensuring that, where internet use is preplanned, pupils only access sites that are checked and have been deemed suitable for their use and that processes are in place to deal with any unsuitable material that is found in internet searches.

Students/Pupils

4.29 Students are responsible for using the ICT systems in accordance with this E-Safety Policy and other Trust policies regarding appropriate use.

4.30 Students need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

4.31 Students should understand the importance of adopting good e-safety practice when using digital technologies inside and out of school and understand that there conduct on digital technology outside of school may be dealt with under the Behavioural Policy within school, where appropriate.

Parents/Carers

4.32 Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate and safe way. Parents/Carers will be responsible for supporting the Trust in following this and the Acceptable Use Policy.

4.34 It is the responsibility of [insert member of staff] to ensure that this policy is up to date and circulated to all staff.

1. **Education and Training**

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

* A planned e-safety programme will be provided as part of the curriculum and will include key e-safety messages appropriate to the age of the pupils.
* Pupils will be taught whenever an opportunity arises regarding awareness of the validity, accuracy and safety of material and content they are accessing online.
* Pupils will be encouraged to adopt safe and responsible practices when using digital technology both within and outside of the academy.
* Staff will act as good role models in their use of digital technology.

Staff/Governor Training:

5.2 All staff and Governors will receive e-safety training and understand their responsibilities as outlined in this policy. Training will be offered regarding e- safety as part of the Level 1 Child Safeguarding Training – Keeping Children Safe in Education.

5.3 All new staff must carry out the Level 1 Child Safeguarding Training and read and agree to the Acceptable Use Policy and read this E-Safety Policy as part of their induction.

1. **Infrastructure, equipment,** **filtering and monitoring**

6.1 The IT Network Manager, IT coordinator and/or IT provider will be responsible for ensuring that the IT systems, infrastructure and network are as safe and secure as is reasonably possible and that policies and procedures are in place and followed to ensure such safety and security.

6.2 All users will have clearly defined access rights to the ICT systems.

6.3 All users will be provided with a username and the user will be required to create a strong, secure password which they will use to access the network.

6.4 Users are responsible for their own username and password and must ensure that they do not allow others to access the system using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security or misuse of their log on details.

6.5 The IT Network Manager, IT Coordinator and/or IT provider will ensure that appropriate filtering systems and firewalls are in place. If these need to be switched off for a particular reason, the Head/Principal must sign off on this beforehand and the reason for switching this off as well as the times/dates must be logged.

6.6 Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager and, where necessary, the Data Protection Officer.

6.7 IT staff/providers regularly monitor and record the activity of users for security purposes.

6.8 Remote management tools may be used by the IT team to control workstations and view user’s activity.

6.9 An appropriate system must be in place to ensure that any e-safety issues can be reported to the E-safety Officer.

6.10 Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices from accidental or malicious attempts which might threaten the security of the IT systems. Staff training is provided regarding IT and Cyber security to avoid user error incidents from occurring.

6.11 Guest users may be granted a guest or temporary log in or account where approved by [insert member of staff.]

6.12 Staff and pupils are only permitted to use the digital technology in line with the appropriate Acceptable Use Policy.

6.13 Personal data (as defined by the Data Protection Act) cannot be sent over the internet or taken off site unless: the data is encrypted or secured by password, the sharing is covered by an appropriate privacy notice and the third party has been approved to receive such information. Please refer to the Data Protection Policy for further information.

1. **Use of digital and video images – photographs/video**

7.1 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. Pupils should be made aware of this in an age-appropriate way.

7.2 There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. Where appropriate, the academy 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 taking, using, sharing, publishing and distributing images. 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 the consent policies concerning the sharing, distribution and publication of those images. Those images should only be taken on 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;
* 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;
* Written permission from parents or carers will be obtained before photographs of students are published on the academy website (this is covered as part of the agreement signed by parents or carers);
* Be aware that downloading, copying or printing images from the internet may also breach copyright laws.

1. **Communications**

8.1 A wide range of rapidly developing communications technologies have the potential to enhance learning, but it is also important to ensure that these technologies are used safely and appropriately.

8.2 Users need to be aware that email and other Trust communication may be monitored and any inappropriate use may lead to action being taken in line with the Behaviour or Disciplinary Policies.

8.3 Users must immediately report any communication received that they perceive to be inappropriate, offensive, threatening or which causes them harassment or distress and must not respond to such communication. In the case of pupils this could be reported to any member of staff. If the staff member receives this communication, it should be reported to a member of the SLT.

8.4 Any digital communication between staff and students or parents / carers (email, e-portal 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;

8.5 Students should be taught about email safety issues, such as the risks attached to the use of personal details and phishing attacks. 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.

1. **Unsuitable/Inappropriate Activities**

9.1 Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from the Trust and all other ICT systems.

9.2 Other activities, e.g. Cyber-bullying, the use of electronic communications to radicalise children or others, is banned and could lead to criminal prosecution.

9.3 There are however a range of activities which may be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. One example would be the use of online gambling sites or other age restricted sites.

1. **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. Schools should ensure that suitable filtering is in place. The Trust monitors the use of digital technology to identify if a user is accessing such content and passes this information to the E-Safety and Safeguarding Officer immediately.

10.2 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. This is covered in the mandatory safeguarding training.

1. **Responding to Incidents of Misuse of Digital Technology**

11.1 All members of the Trust community will be responsible for understanding and following this policy. There may, however, be times when infringements of this policy take place, either through carelessness, irresponsible behavior or, in rare cases, deliberate misuse.

11.2 If such careless, irresponsible or deliberate misuse occurs, the Trust will respond accordingly. The response will depend on the nature of the misuse. Some information is provided below regarding the appropriate action to take for certain types of misuse:

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 matter must be reported to the Head/Principal or Chair of Governors/COO as necessary immediately. The Head/Principal or Chair of Governors/COO must inform the relevant authorities immediately. If such material was accessed/sent by a child under the age of criminal responsibility (under 10 years old) the Head/Principal must liaise with the DSL and take any appropriate steps under the Safeguarding Policy.

If any apparent or actual misuse appears to involve cyber-bullying

This matter should be reported to the E-Safety Officer and recorded in writing and dealt with in line with the school/Trust’s behaviour policy.

If the misuse involves revealing or sharing personal information

This should be reported to the Head/Principal and your Data Protection Officer as soon as possible. This may be a data breach and may need to be reported to the Information Commissioners Office. If it is, this will need to be reported within 72 hours of discovery, so it is important to inform the DPO immediately.

1. **Complaints**

12.1 Any complaints about this policy, its use or implementation should be addressed to the [insert details].

1. **Breaches of this policy**

13.1 Any breach of this policy should be dealt with in accordance with clause 11 above.

1. **Review**

14.1 This policy should be reviewed biennially.

This policy was last updated on: [insert the date].