# E Safety Policy

**Date: September 2024**

**Review Date: September 2026**

1. Aims

New technologies inspire young people to be creative, communicate and learn. Whilst the internet is a great resource, it is important that young people are protected from the risks they may encounter and how to be safe online. Navigators will highlight benefits and risks of using technology and provide Safeguarding and education for users to enable them to control their online experience. The following Navigators policies and procedures should also be referred to;

- Safeguarding Policy
- Whistleblowing policy
- Supporting Behaviour Policy
- Staff code of conduct
- Information Sharing Policy

The following local/national guidance should also be read in conjunction with this policy:

- PREVENT Strategy HM Government
- Keeping Children Safe in Education DfE September 2024
- Teaching Online Safety in Schools DfE June 2019
- Working together to Safeguard Children
- Learning together to be Safe: A Toolkit to help Schools contribute to the Prevention of Violent Extremism Implementation

2. Learning & Teaching

We believe that it is essential to develop attitudes to safe and responsible behaviours online, not only for students but everyone within our orgaisations community. We know that the internet and other technologies are embedded in our students lives, not just in Navigators but outside as well. We have:

- have a duty to help prepare our students to safely benefit from the opportunities the internet brings.
- We will provide a curriculum which has e-Safety related lessons embedded throughout.

● We will celebrate and promote e-Safety through a planned sessions in our PCD curriculum.

● We will discuss, remind or raise relevant e-Safety messages with students routinely wherever suitable opportunities arise during all sessions including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.

● Any internet use will be carefully planned and monitored to ensure that it is age appropriate and supports the learning objective for specific curriculum areas.

● Students will be taught how to use a range of age-appropriate online tools in a safe and effective way.

● We will remind pupils about their responsibilities through an Acceptable Use Policy which every student will sign.

● Students will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-Bullying Policy.

3. Remote/Home Learning - (Please also see remote learning policy).

We will endeavour to ensure that students continue to receive a good level of education ‘beyond the classroom’ by providing a range of resources via our website and Microsoft teams. We expect students to follow the same principles, as outlined in the organisations Acceptable Use policy, whilst learning at home. Any significant behavioural issues occurring on any virtual platform must be recorded, reported and appropriate sanction imposed, which may include temporarily suspending access to online learning. For all minor behavioural incidents, these should be addressed using the normal restorative approaches.

4. General Note for Incidents in person or online

● At every stage the child should be involved in or informed of the action taken

● Urgent or serious incidents should be referred straight to the DSL/DDSL

● If necessary, refer to the other related internal policies eg Anti-Bullying, Child Protection, ESafety etc

● Normal recording systems on CPOMS should continue.

5. Staff Training

Navigators staff receive regular information and training on e-Safety issues, as well as updates as and when new issues arise. As part of the induction process all staff receive information and guidance on the Online Safety Policy, Navigators Acceptable Use Policy, e-security and reporting procedures. All staff will be 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 Navigators community.

6. Managing ICT Systems and Access

Navigators will agree on which users should and should not have internet access and the appropriate level of access and supervision they should receive.

● All users will sign an Acceptable Use Policy provided by the organisation, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using Navigators ICT system and that such activity will be monitored and checked.

● All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.

● Members of staff will access the internet using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID or password.

## 7. Managing Filtering

The Organisation has a filtering system in place which is managed by the organisation. Banned phrases and websites are identified. Navigators have a clearly defined procedure for reporting breaches of filtering. If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator immediately. If users discover a website with potentially illegal content, this should be reported immediately to the e-Safety Coordinator. The Organisation will report such incidents to appropriate agencies including Internet Service Provider (ISP), Police, CEOP or the Internet Watch Foundation (IWF).

## 8. E-mail

Staff should only use approved email accounts allocated to them by the organisation for their professional work, and should be aware that any use of Navigators email system will be monitored and checked. Staff should not use personal email accounts for professional purposes, especially to exchange any business related information or documents or to email parents/carers.

## 9. Social Networking

Staff will not post content or participate in any conversations which will be detrimental to the image of the organisation. Staff who hold social media accounts should not have students as their ‘friends’. Doing so could result in disciplinary action or dismissal. All pupils will have consent before any images of them are shared on our website or social media.

## 10. Students Publishing Content Online

Students will not be allowed to post or create content on sites unless the site has been approved by a member of staff. Students full names will not be used anywhere on the website, particularly in association with photographs and video.

11. Screening, Searching and Confiscation

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by organisation rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- commit an offence,
- cause personal injury,
- or damage property.

Please see Navigators 'Supporting Pupils with Behaviour Policy' for further details.

12. CCTV

Navigators may use CCTV in some areas the organisation's properties as a security measure. Cameras will only be used in appropriate areas and there is clear signage indicating where it is in operation.

13. General Data Protection (GDPR) & e-Safety

Data will always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected. GDPR is relevant to e-safety since it impacts on the way in which personal information should be secured on organisational networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material. Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the organisation population and external stakeholders, particularly, but not exclusively: students, parents, staff and external agencies. Personal and sensitive information should only be sent by

email when on a secure network – Navigators use egress. Personal data should only be stored on secure devices. In the event of a data breach, HR will notify the Trust's Data Protection Officer (DPO) immediately, who may need to inform the Information Commissioner's Office (ICO).

14. Authorising Internet Access

All staff must read and sign the 'Acceptable Use Policy' before using any Navigators ICT resources. All parents will be required to sign the agreement prior to their children being granted internet access within sessions. They will be issued with their own temporary usernames and passwords for internet access.

15. Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the DSL / DDSL). Regular monitoring and filtering is in place to ensure that access to appropriate material on the internet and key word reporting is in place to ensure safety for all staff and pupils.

16. Sexual Harassment

Sexual Harassment Sexual harassment is likely to: violate a young persons dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment. Online sexual harassment, which might include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats). Please refer to Sexual Harassment Policy

17. Responses to Incidents of Concern

An important element of e-Safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff, volunteers and students have a responsibility to report e-Safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact. Navigators has incident reporting procedures in place and staff should record incidents of an e-Safety nature on CPOMS.

18. Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or expulsion, in accordance with the organisations Supporting Students Behaviour Policy. The organisation also reserves the right to report any illegal activities to the appropriate authorities. Policy review will take place as and when changes are necessary to comply with Navigators policy or national legislation.

**Appendix 1**

All Staff, Student (non-pupil) and Volunteer Acceptable Use Policy New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for students/volunteers to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times. This Acceptable Use Policy is intended to ensure:

● that all adults will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

● that Navigators systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

● that all adults are protected from potential risk in their use of technology in their everyday work. The school will try to ensure that adults will have good access to digital technology to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect students / volunteers to agree to be responsible users.

Acceptable Use Policy Agreement I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people. For my professional and personal safety:

● I understand that Navigators will monitor my use of the school digital technology and communications systems.

● I understand that the rules set out in this agreement also apply to use of these technologies (e.g. Microsoft teams) out of school, and to the transfer of personal data (digital or paper based) out of school.

● I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

● I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

● I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

• I will be professional in my communications and actions when using Navigators ICT systems.

● I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

● I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

● I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

● I will not engage in any on-line activity that may compromise my professional responsibilities. The school and Local Authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school.

● When I use my mobile devices (laptops / tablets / mobile phones) at Navigators I will follow the rules set out in the organisations E-Safety Policy, in the same way as if I was using school equipment.

● I will not use personal email addresses on the school ICT systems without seeking permission.

● I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

● I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

● I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

● I understand that data protection policy requires that any pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

● Where work is protected by copyright, I will not download or distribute copies (including music and videos). I understand that I am responsible for my actions in and out of the school.

● I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

● I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the Disciplinary Committee and in the event of illegal activities the involvement of the police. I have read and understand the above and agree to use the school digital technology systems (both in and

out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name : …….

Position in organisation: …….

Signed: …….

Date: …….

**Appendix 2**

**Pupil Acceptable Use Policy Agreement**

(Parents / carers consent to this AUP when their child joins the school. Children are reminded of these principles regularly and they are clearly displayed in classrooms).

This is how we stay safe when we use computers:

● I will ask a mentor or suitable adult when I want to use a device

● I will only use appropriate online material that a member of staff or suitable adult has told or allowed me to use

● I will take care of the computer and other equipment

● I will ask for help from a member of staff or suitable adult if I am not sure what to do or if I think I have done something wrong.

● I will tell a member of staff or suitable adult if I see something that upsets me on the screen.

● I know that if I break the rules I might not be allowed to use a computer.

• I will not use inappropriate language when communicating digitally.

• I will not access any inappropriate materials and understand the consequences if I do.

Signed ……

**Appendix 3 Parent/Carer Acceptable Use Policy Agreement**

(Parents / carers consent to this AUP when their child joins the school)

As the parent / carer of a Navigators Student I give permission for my son / daughter to have access to the internet and to ICT systems at school.

● I know that my son / daughter has seen and agreed to an Acceptable Use Agreement and has received, or will receive, regular e safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

● I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

● I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

● I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety

Signed …….. (parent/carer)