RAISE
EDUCATION TRUST

Initial Policy:	Feb 2016
Policy Updated:	Jul 2024
Next Review:	Jul 2025
Key Person:	JBW

RAISE EDUCATION TRUST

E-Safety Policy

Principles

- To ensure that all members of the school community are E-Safety conscious and understand how to protect themselves online.
- RAISE Education Trust seeks to protect children and young people against the messages of all violent extremism, including, but not restricted to, those linked to extreme Islamist ideology, or too Far Right / Neo Nazi / White Supremacist ideology, Irish Nationalist and Loyalist paramilitary groups, and extremist Animal Rights movements (See the Preventing Extremism and Radicalisation policy).

Practice

- All Year groups are regularly taught E-Safety in order to keep abreast of online developments enabling them to stay safe online.
- Within the E-Safety lessons for students and staff throughout the year an evolving scheme of work (SOW)/Training schedule will be delivered looking at radicalisation and extremism, and indicators of vulnerability to radicalisation. This is to ensure that the values of freedom of speech and the expansion of beliefs / ideology as fundamental rights underpinning our society's values are valued.
- Annually all staff, Trustees and Local Governors have E-Safety training on how to maintain safety on-line.
- Annually parents are invited to a WINK event on E-Safety on how to ensure they know and understand how to keep themselves and their children safe on-line.

Passwords

RAISE Education Trust staff / Members, Trustees and Local Governors:

- Will be provided with a username and password.
- The password should be a minimum of 14 characters long and must include at least one Capital Letter, number and special character. (!"£$%^&*)
- The password must not include proper names or any other personal information about the user that might be known by others.
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption).
- Staff will not use the same password for multiple accounts.
- Staff to set up two factor authentication on accounts email, pars and insight

Student passwords

- All users will be provided with a username and password.
- Password security: The password should be a minimum of 8 characters long and must include letters and numbers.

Bring your own device (BYOD)

The educational opportunities offered by mobile technologies are expanding as a wide range of devices, software, and online services become available for teaching and learning within and beyond the classroom. RAISE Education Trust has explored, like many schools, users bringing in their own technologies in order to provide a greater freedom of choice and usability at the same time as not introducing vulnerabilities into existing secure environments.

- The school has a set of clear expectations and responsibilities for all users of BYOD.
  - The school adheres to the Data Protection Act principles and (referred to in the General Data Protection Regulation (GDPR).
  - All users are provided with and accept the Acceptable Use Policy Agreement.
  - All network systems are secure and access for users is differentiated.
  - Where possible these devices will be covered by our normal filtering systems, while being used on the premises.
  - All users will keep their login credentials private.
  - All staff undertake mandatory training.
  - Students receive training and guidance on the use of personal devices.
  - Regular audits and usage monitoring will take place to ensure compliance.
  - Any device loss, theft, or change of ownership of the device will be reported to IT Support.

Cyber-bullying

RAISE Education Trust embraces the advantages of modern technology in terms of the educational benefits it brings, however the school is mindful of the potential for bullying to occur. Central to the Trust's anti-bullying policy is the belief that 'all students have a right not to be bullied' and that 'bullying is always unacceptable'.

The Trust also recognises that it must 'take note of bullying perpetrated outside School which spills over into the School'. Under powers granted by the EIA (Education and Inspections) 2006, the CEO/Headteacher is able to police cyber-bullying or any bullying aspects carried out by students even at home.

The school actively scans students' online storage and emails for signs of Cyberbullying. Any occurrences are passed to year DOPAs for action

Definition of cyber-bullying

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend themselves.

By cyber-bullying, we mean bullying by electronic media such as:

- Bullying by texts or messages or calls on mobile phones.
- The use of mobile phone cameras to cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites.
- Using e-mail to message others.
- Hijacking/cloning e-mail accounts.
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms, to include Facebook, Bebo, Youtube and Ratemyteacher and the like.

Legal issues

Cyber-bullying is not a specific offence but may in some instances be contrary to the civil or criminal law. In particular:

- It is unlawful to disseminate defamatory information in any media including internet sites.

- Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.
- The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.
- Section 1 of the Malicious Communications Act 1988 makes it an offence to send an electronic communication which is indecent or grossly offensive, or which conveys a threat, or which is false where there is an intention to cause distress or anxiety to the recipient.

Practice

- The Trust educates its students both in the proper use of telecommunications and about the serious consequences of cyber-bullying and will, through ICT (Information Communication Technology) lessons and assemblies, continue to inform and educate its students in these fast changing areas.

- The Trust trains its staff to respond effectively to reports of cyber-bullying or harassment and has systems in place to respond to it.

- The Trust endeavours to block access to inappropriate websites, using firewalls, antivirus protection and filtering systems and no student is allowed to work on the internet in the Computer Room, or any other location within the school which may from time to time be used for such work, without a member of staff present.

- Where appropriate and responsible, the Trust audits ICT communications and regularly reviews the security arrangements in place.

Whilst education and guidance remain at the heart of what we do, we reserve the right to take action against those who take part in cyber-bullying.

- All bullying is damaging but cyber-bullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts.

- The Trust supports victims and, when necessary, will work with the Police to detect those involved in criminal acts.

- The Trust will use, as appropriate, the full range of sanctions to correct, punish or remove students who bully fellow students or harass staff in this way, either in or out of school.

- The Trust will use its power of confiscation where necessary to prevent students from committing crimes or misusing equipment.

- All members of the Trust's community are aware they have a duty to bring to the attention of the CEO/Headteacher any example of cyber-bullying or harassment that they know about or suspect.

Responsibilities in each school

Deputy Headteacher will:

- Liaise with the SLC (Communication Studies) ICT, E-Safety Co-ordinator and Assistant Headteacher for ICT and School IT Systems in order to be updated regarding E-Safety developments which will affect the school community, curriculum, staff training.

Assistant Headteacher for ICT and School IT Systems will:

- Keep abreast of any developments pertaining safety / E-Safety of the network and curriculum and advise the Deputy Headteacher accordingly.
- Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Provides training and advice for staff.

- Liaises with the Local Authority / relevant body when applicable.
- Liaises with school technical staff.
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments.
- Meets regularly with Safeguarding Governor to discuss current issues.

SLC (Communication Studies) will:

- Keep abreast of ICT / E-Safety developments pertaining to their subject in order to maintain high quality learning and teaching as well as safety across the school.
- Liaise with the E-Safety Co-ordinator regularly for updates.

IT Manager will:

- Keep abreast of ICT / E-Safety developments pertaining to the network in order to maintain high quality safety across the school.
- Liaise with the Headteacher and School IT Systems regularly for updates.
- Monitor the automated e-safety monitoring system and report issues to year heads.

E-Safety Coordinator

- Leads the E-Safety student focus group.
- Reports regularly to Senior Leadership Team.

An SLT (Senior Leadership Team) Member of Staff with responsibility for E-Safety will link via the SLC ICT to the E-Safety Coordinator for updates and any further training required for students, staff, parents and Governors.

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding E-Safety and monitoring the E-Safety policy including the impact of initiatives.

Members of the E-Safety Group will assist the E-Safety Coordinator with:

- o The production / review / monitoring of the school E-Safety policy / documents.
- o Mapping and reviewing the E-Safety curricular provision – ensuring relevance, breadth and progression.
- o Monitoring network / internet / incident logs.
- o Consulting stakeholders – including parents / carers and the students about the E-Safety provision.
- o Monitoring improvement actions identified through use of the 360 degree safe self-review.

Staff

- To be aware of E-safety of themselves on-line and also regarding the students at the school.
- To make sure they are up to date with their information regarding E-safety.

Appendix 1: Guidance on Cyber bullying

a) Staff

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Mobile Phones

- Ask the student to show you the mobile phone.
- Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names.
- Make a transcript of a spoken message, again record date, times and names.
- Tell the student to save the message/image.
- Inform a member of the Senior Leadership team and pass them the information that you have.

Computers

- Ask the student to get up on-screen the material in question.
- Ask the student to save the material.
- Print off the offending material straight away.
- Make sure you have got all pages in the right order and that there are no omissions.
- Inform a member of the Senior Leadership team and pass them the information that you have.
- Normal procedures to interview students and to take statements will then be followed particularly if a child protection issue is presented.

b) Students

If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, or a member of staff at your School.

- Do not answer abusive messages but save them and report them.
- Do not delete anything until it has been shown to your parents/guardian or a member of staff at your school (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying).
- Do not give out personal IT details.
- Never reply to abusive e-mails.
- Never reply to someone you do not know.
- Stay in public areas in chat rooms.

c) Parents

It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. RAISE EducationTrust informs parents of the cyber-bullying policy and the procedures in place to deal with cyber-bullying.

- Parents can help by making sure their child understands the school's policy and, above all, how seriously RAISE Education Trust takes incidents of cyber-bullying.
- Parents should also explain to their children legal issues relating to cyber-bullying.
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything.
- Parents should contact the school as soon as possible. A meeting can then be arranged with a member of the Senior Leadership Team.
- If the incident falls in the holidays RAISE Education Trust reserves the right to take action against bullying perpetrated outside the school which spills over into the school.

E-Safety at home

Several sites offer helpful advice to parents, particularly with respect to how they can best monitor their child’s use of the computer at home. Important and useful information can be found on the following sites:

http://wilderne-safety.blogspot.co.uk/

https://www.wildern.hants.sch.uk/news/ceop/

https://www.deerparksecondary.org/news-and-social-media/esafety-and-ceop/

Linked Policies :

Anti-Bullying Policy
British Value Statement
Child Protection Policy
Complaints Policy
Code of Conduct
Data Protection Policy
Education for Life
Information Communication Technology (ICT) Policy
Preventing Extremism and Radicalisation
Safeguarding Policy
Whistleblowing (Protected Disclosures) Policy