Victoria Road Primary School E-Safety Policy

Policy written by	Tracey Taylor
Reviewed	September 2023
Next Review	September 2024
Head teacher	Mrs Emma Roberts
Chair of Governors	Mrs Hilary Moss

Signed:... Head Teacher

Signed:... Chair of Governors

Victoria Road Primary School E-Safety Policy

Responsibilities

The members of school staff responsible for e-safety are: **Mrs Emma Roberts & Mrs Tracey Taylor**

They are responsible for delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety within the school community.

The designated member of staff for Prevent is Mrs Emma Roberts

The E-Safety policy is read in accordance with the Acceptable Use Policies

The Prevent Duty

The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism. The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet. The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

Schools should ensure that suitable filtering is in place. More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's Computing curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

The Prevent Duty requires a schools monitoring and filtering systems to be fit for purpose.

Online Safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

- contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying

Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents is gained if videos or photos of pupils are going to be used. If photos/videos are to be used publicly online and on social media then names of pupils should not be linked to pupils.

Staff must be fully aware of the consent form responses from parents when considering use of images. This is updated annually as part of the data collection exercise. Staff should always use a school ipad to capture images and should not use their personal devices unless as stated below.

Photos taken by the school are subject to the Data Protection Act.

Photos and videos taken by parents/carers.

Parents and carers are permitted to take photos of their own children in school events. They are requested not to share photos from school events on social networking sites if other pupils appear in the background. Parents attending school based events will be reminded of their responsibilities in relation to social media verbally and through notices. Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

Mobile phones and other devices

Victoria Road Primary School recognises that staff may need to have access to mobile phones on site during the working day. However, there have been a number of queries raised within the local authority and nationally regarding the use of mobile phones and other devices in educational settings. The concerns are mainly based around these issues:

- Staff being distracted from their work with children

- The use of mobile phones around children

- The inappropriate use of mobile phones

Ensuring the Safe and Appropriate Use of Mobile Phones

Victoria Road Primary School allows staff to bring in mobile phones for their own personal use. However, they must be kept securely at all times and are not allowed to be used during teaching hours and an areas where children are present. If staff fail to follow this guidance, disciplinary action will be taken in accordance to the school’s staff code of conduct.

In very rare circumstances if a staff member is waiting for an important call, then they are allowed their phone on during class time with the Headteacher’s permission.

Staff must ensure that there is no inappropriate or illegal content on the device. Members of staff may only contact a parent/carer on school approved mobile phones, making sure you use ‘No caller ID’.

Pupils should not use mobile phones within the school grounds and should not bring in a mobile to school unless they are walking home from school alone and then the mobile will be switched off and handed to the school office/class teacher at the start of the school day and collected at home time.

We believe that photographs validate children’s experiences and achievements and are a valuable way of recording milestones in a child’s life. Parental permission for the different ways in which we use photographs is gained as part of the initial registration at this school. We take a mixture of photos that reflect the school environment; sometimes this will be when children are engrossed in an activity either on their own or with their peers. In order to safeguard children and adults and to maintain privacy, ipads are not to be taken into the toilets by adults or children.

All adults whether teachers/practitioners or volunteers at the school understand the difference between appropriate and inappropriate sharing of images. All images are kept securely in compliance with the Data Protection Act. If a member of staff suspects that any device has been misused within the school, then the whistle blowing/ safe guarding procedure will be adhered to. A senior member of staff will confiscate the device and keep it in a securely locked place.

Use of e-mails

Security and passwords Passwords should be changed regularly. The system will inform users when the password is to be changed. Passwords must not be shared. Staff must always ‘lock’ the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be ‘locked’). All users should be aware that the ICT system is filtered and monitored.

Data storage

Only encrypted USB pens are to be used in school. All staff should use the Google Drive to store and retrieve school information.

Reporting

All breaches of the e-safety policy need to be reported to the Headteacher. The details of the user, date and incident should be reported. Incidents which may lead to child protection issues need to be passed on to the Headteacher/Designated Safeguarding Lead immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents that are of a concern under the Prevent duty should be referred to the designated lead immediately who should decide on the necessary actions regarding safeguarding and the Channel Panel.

Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to SLT in the same day. Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled ‘Dealing with allegations of abuse against teachers and other staff’. If necessary the local authority’s LADO should be informed. Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, ChildLine).

Infringements and sanctions

Whenever a student infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school . The following are provided as exemplification only:

Level 1 infringements:-

• Use of non-educational sites during lessons

• Unauthorised use of email Use of unauthorised instant messaging / social networking sites [Possible Sanctions: referred to class teacher / e-Safety Coordinator/ confiscation of device]

Level 2 infringements:-

• Continued use of non-educational sites during lessons after being warned

• Continued unauthorised use of email after being warned

• Unauthorised use of device.

• Continued use of unauthorised instant messaging / social networking sites

• Use of File sharing software

• Accidentally corrupting or destroying others' data without notifying a member of staff of it

• Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to Class teacher/ e-safety Coordinator / removal of

Internet access rights for a period / confiscation of device / contact with parent]

Level 3 infringements:-

- Deliberately corrupting or destroying someone’s data, violating privacy of others
- Sending an email or message that is regarded as harassment or of a bullyingnature (one-off)
- Deliberately trying to access offensive or pornographic material

[Possible Sanctions: referred to Class teacher / e-safety Coordinator / Headteacher / removal of Internet rights for a period / contact with parents] Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site

2. Inform SSCB/LA as appropriate

Level 4 infringements

• Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned

• Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent

- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act.

- Bringing the school name into disrepute

[Possible Sanctions – Referred to Head Teacher / Contact with parents / possible

exclusion / refer to Community Police Officer / LA e-safety officer]

Other safeguarding actions:

1. Secure and preserve any evidence

2. Inform the sender's e-mail service provider if a system other than the school system is used.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Social networking

Pupils are not permitted to use social networking sites within school.

E-Safety Education

Pupils

To equip pupils as confident and safe users of ICT the school will undertake to provide:

a). A planned, broad and progressive e-safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years.

b). Regularly auditing, review and revision of the computing curriculum

c). E-safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner

d). Opportunities for pupils to be involved in e-safety education e.g. through peer mentoring, e-safety officers, parent presentations etc The e-safety officers get trained and give out e safety advise in assembly.

Additionally,

a). Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information

b). There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

c). The school actively provides systematic opportunities for pupils / students to develop the skills of safe and discriminating on-line behaviour

d). Pupils are taught to acknowledge copyright and intellectual property rights in all their work.

Staff

a). In order to ensure that staff are aware of the E-safety risk, relevant to their role for both themselves and the teaching and learning of children, staff will complete yearly certificated training. Our current training is provided by NSPCC and Schoot. Additionally, all staff will have Home Office training on the Prevent duty.

b). E-safety training is an integral part of Child Protection / Safeguarding training and vice versa

c). All staff have an up to date awareness of e-safety matters, the current school e- safety policy and practices and child protection / safeguarding procedures

d). All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use

Policy

e). The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety

f). The school takes every opportunity to research and understand good practice that is taking place in other schools

g). Governors are offered the opportunity to undertake training.

Parents and the wider community

There is a programme of e-safety sessions for parents, carers, etc. The O2 Gurus, Vodafone, National Online Safety and Family Learning will provide guidance on this matter.

Monitoring and reporting

a). The school network provides a level of filtering and monitoring that supports safeguarding.

b). The impact of the e-safety policy and practice is monitored through the review / audit of e-safety incident logs, behaviour / bullying logs, surveys of staff, students / pupils, parents / carers

c). The records are reviewed / audited and reported to:

- the school’s senior leaders

- Governors

- Halton Local Authority (where necessary)

- Halton Young People’s Safeguarding Partnership

d). The school action plan indicates any planned action based on the above.