DIGITAL SAFEGUARDING POLICY

September 2018

Designated Safeguarding Lead: Tracy Harper

Statement of Intent

At Thurcroft Infant School we understand that computer technology is an essential resource for supporting teaching and learning.
The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.
Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.
This policy has the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.
The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

Legal framework This policy has due regard to statutory legislation, including, but not limited to, the following: This policy has due regard to the following legislation, including, but not limited to:

 The Human Rights Act 1998 The Data Protection Act 1998 The Regulation of Investigatory Powers Act 2000 The Safeguarding Vulnerable Groups Act 2006 The Education and Inspections Act 2006 The Computer Misuse Act 1990, amended by the Police and Justice Act 2006 This policy also has regard to the following statutory guidance:

 DfE (2016) 'Keeping children safe in education' Prevent Guidance for schools 2015

Use of the internet
The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

Internet use is embedded in the statutory curriculum and is therefore an entitlement to all pupils, though there are a number of controls the school is required to implement to minimise harmful risks. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Acess to illegal, harmful, inappropriate images
- Cyber bullying
- Access to or loss of personal information
- Access to unsuitable online videos or games
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to harmful content involving radicalisation
- Plagiarism and copyright infringement
- Youth Produced Sexual Imagery (YPSI) or 'sexting'

Portable Equipment

The school provides portable ICT equipment such as laptop computers, Ipads and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities. No further equipment should be brought in from the pupils as it is not required on premises.
No portable equipment or devices will be used to harm or embarrass another person.
No portable equipment or devices will be used to bully or intimidate another person.
Equipment such as laptop computers are encouraged to be taken offsite for use by staff in accordance with the Staff Code of Conduct.
Staff are required to sign a disclaimer accepting full responsibility for the equipment in their care, and that the equipment is fully insured from the moment it leaves the academy premises.
No files should be transported off the site on a memory stick, laptop or similar that contain any personal information about a pupil or staff including a pupil or staff's full name.
All files leaving the site should be encrypted and should only be accessible using a 'strong' password.

Roles and responsibilities

It is the responsibility of all staff to be alert to possible harm to pupils or staff, due to inappropriate internet access or use, both inside and outside of school, and to deal with incidents of such as a priority.

The external ICT contractor is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

Headteacher/Head of School is responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this Digital Safeguarding Policy.

Parents of pupils are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

The Head of School/Headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

E-safety control measures

Educating pupils:

Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material.

Pupils will be taught to acknowledge information they access online.

Pupils are instructed to report any suspicious use of the internet and digital devices.

Educating staff:

All staff will undergo e-safety training on a regular basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.

All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

All staff will be educated on which sites are deemed appropriate and inappropriate. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this Digital Safeguarding Policy.

Internet access:
Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
Effective filtering systems will be established to eradicate any potential risks to pupil's inappropriate material.
Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of IT systems, and the proportionality of costs compared to risks.
All school systems will be protected by up-to-date virus software.
An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only, and no personal devices. This will be dealt with following the process outlined in this policy.

Email:
Staff will be given approved email accounts and are only able to use these accounts.
No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
Chain letters, spam and all other emails from unknown sources will be deleted without opening.

Social networking:
Access to social networking sites will be filtered as appropriate.
Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Head of School/Headteacher.

Pupils are regularly educated on the implications of posting personal data online, outside of the school.
Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
Staff are not permitted to publish comments about the school which may affect its reputation.
Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the Head of School/Headteacher prior to accessing the social media site.

Published content on the website and images:
Contact details on the website will include the phone number, email and address of the school.
No personal details of staff or pupils will be published.
Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.

Pupils are not permitted to take or publish photos of others without permission from the individual.
Staff are able to take images, though they must do so in accordance with school policies in terms of the sharing and distribution of such.
Staff will not take images using their personal equipment.
Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

Mobile devices and hand-held computers:
Mobile devices are not permitted to be used during school hours by pupils or members of staff.
Staff are permitted to use hand-held computers which have been provided, though internet access will be monitored for any inappropriate use.
The sending of inappropriate messages or images from mobile devices is prohibited.
Mobile devices will not be used to take images or videos of pupils or staff.
The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

Virus management:
Technical security features, such as virus software, are kept up-to-date and managed by the school Esafety officer.

Cyber bullying For the purpose of this policy, "cyber bullying" is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.
The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

We will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.
Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE.
We will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying and Harassment Policy.

Youth Produced Sexual Imagery (YPSI) – 'sexting' 'Sexting' is one of a number of 'risk-taking' behaviours associated with the use of digital devices, social media or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with 'online' activity can never be completely eliminated.