Filtering and Monitoring Training

Clee Hill Community Academy – September 2023

Training for all staff and volunteers

You should identify and assign roles and responsibilities to manage your filtering and monitoring systems

- Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.
- Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It's important that the right people are working together and using their professional expertise to make informed decisions.
- Ceri Little, headteacher and Computing lead, alongside the governing body, is responsible to check that filtering and monitoring systems are robust. Our link governor for Safeguarding is Mary Bland.

As part of this role, I am responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

I am also responsible for making sure that all staff and volunteers:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

All staff, parents and pupils agree to our AUP each year. Also, our E-Safety policy which is read and signed each year by all staff includes a section on filtering and monitoring which states:

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content Online/E-Safety Policy - lists are regularly updated and internet use is logged and regularly monitored.). There is a clear process in place to deal with requests for filtering changes
- The school has enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)
- Trust technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Temporary access of “guests” can be facilitated (e.g. trainee teachers, supply teachers, visitors) onto the school systems but these guests must comply with the contents of this policy.
- Personal data (as defined in GDPR) cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- http://lacon-childe.org.uk/media/45139/onlinee-safety-september-2022.pdf

Monitoring - SENSO

In addition to our filtering system, we also use a safeguar called SENSO. Senso. cloud is a software that provides an enhanced level of management, enabling teachers and network managers to monitor and manage off-line computer activity in schools.

Every time a child logs into a device, it reviews the content and reports any concerns to the designated safeguard lead, Ceri Little.

Trigger words or actions are screenshot and sent to the email of the DSL. The children are aware of this – ie during WW2 topics, the word ‘bomb’ might trigger an email.

SENSO provides information of any pupils who may try to access inappropriate material in school when logged into a device.

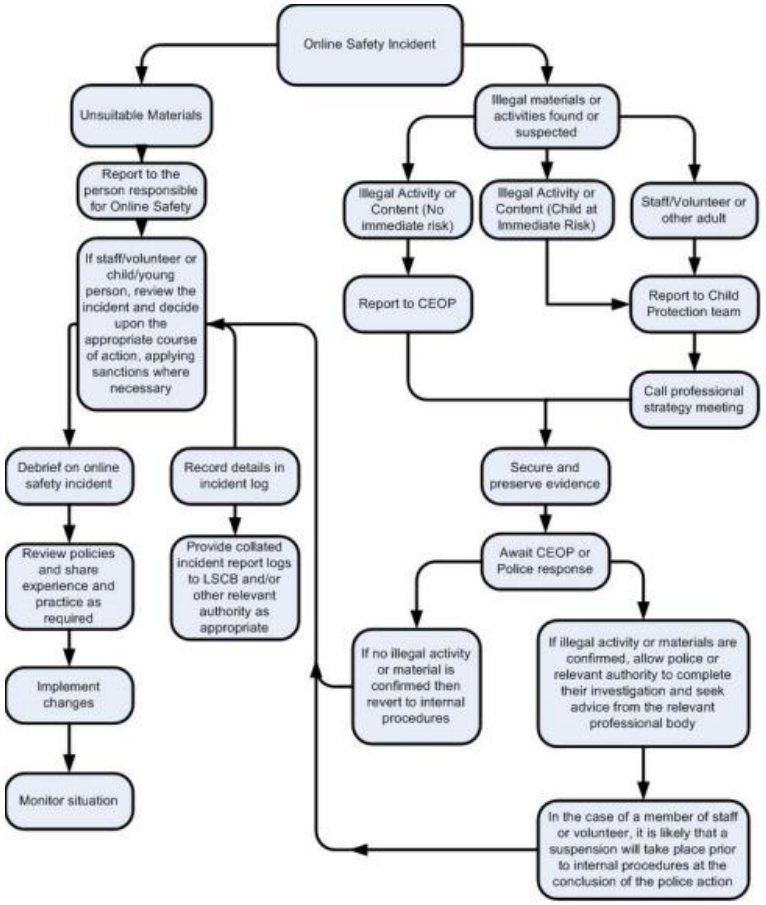
Radicalisation and the Use of Social Media to encourage extremism

Shropshire Gateway Educational Trust has a number of measures in place to help prevent the use of Social Media for this purpose: · Web site filtering is in place, and can be put in place, as appropriate to help prevent access to terrorist and extremist material and social networking sites (e.g Facebook, Instagram or Twitter) · Pupils, Parents and Staff are educated in safe use of Social Media and the risks posed by on-line activity, including from extremist and terrorist groups

Use of digital and video images

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. Mobile phones can not be used in areas of the school where children are present without the authorisation of the Headteacher.

Reporting Concerns of misuse



On page 15 of the E Safety policy there is a clear diagram of how to report any misuse. A copy of this table can also be found on the computing display board in the Computer Suite.
The children are taught about CEOP as part of our Internet Safety Curriculum, in assemblies and through the digital leader assemblies.

Our designated safeguard leads are:

Ceri Little
Hattie Barnes
Donna Richardson