Filtering and Monitoring

Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system". However, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

What is filtering and monitoring?

Filtering systems block access to harmful websites and content. Monitoring systems identify when someone searches for or accesses certain types of harmful online content on school devices, identify who is searching for or accessing the harmful content and alerts the school about it so we can intervene and respond

Decision Making

- Governors and Leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place to limit learners' exposure to online risks.
- Governors and Leaders are aware of the need to prevent "over blocking" as that may unreasonably restrict what can be taught with regards to online activities and safeguarding.
- Changes to the filtering and monitoring approach will be risk assessed by the Leadership Team. All changes to the filtering policy are logged and recorded.
- The Leadership Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners. Effective classroom management and regular education about safe and responsible use is essential.

Filtering

- Education broadband connectivity is provided through Virgin Media Business.
- We use Meraki Firewall which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. We also are aware of the filtering detecting other safeguarding issues, such as self-harm, serious violent crime or issues with county lines grooming.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- Content lists are regularly updated
- The school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges

- All school devices are connected to a filtered feed. If a school device needs access to additional content, for instance to manage official social media, the filter settings for that device or user should be modified to allow access to that content once the Headteacher has been consulted.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes
- Any material believed to be illegal will be reported immediately to the appropriate agencies.

Monitoring

- The school uses Senso Safeguard Cloud to monitor all network use across all its devices and services.
- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - Physical monitoring (supervision), monitoring internet and web access.
    - Alerting e-mails are sent to the Headteacher who then takes appropriate action.
- If a concern is identified via monitoring approaches:
    - Headteacher will respond in line with the Child Protection policy.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These include:

- physical monitoring
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to Leadership Team