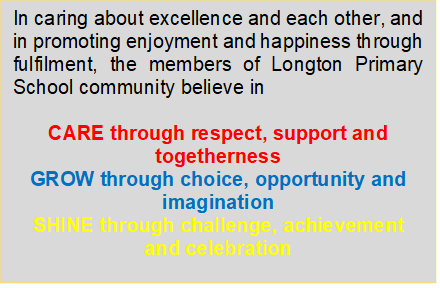
### **Background pattern Description automatically generated**



### A picture containing background pattern Description automatically generated**Filtering Policy**

36

#### Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

### Responsibilities

The responsibility for the management of the school’s filtering policy will be held by Deputy Headteacher. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must

* **be logged in change control logs**
* **be reported to a second responsible person** Headteacher

All users have a responsibility to report immediately to the Deputy Headteacher any infringements of the school’s filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

### Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

* The school manages its own filtering service Netsweeper provided by the Service Provider BTLS
* The school has provided enhanced/differentiated user-level filtering through the use of the Netsweeper filtering programme. (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/
* Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
* Any filtering issues should be reported immediately to the filtering provider.
* Requests from staff for sites to be removed from the filtered list will be considered by the Deputy Headteacher If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

### Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

* the acceptable use agreement
* induction training
* staff meetings, briefings, Inset.

A picture containing background pattern

Description automatically generatedParents will be informed of the school’s filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter.

### Changes to the Filtering System

In this section the school should provide a detailed explanation of:

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to Deputy Headteacher will decide whether to make school level changes (as above).

### Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school online safety policy and the acceptable use agreement. Monitoring will take place as on a monthly rota by the technician and Deputy Head

### Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to the Headteacher.

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

### Further Guidance

35

School may wish to seek further guidance. The following is recommended:

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" ([Revised Prevent Duty Guidance: for England and Wales, 2015](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf)).

The Department for Education ‘[Keeping Children Safe in Education’](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)requires schools to: “ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges 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.”

In response UKSIC produced guidance on – information on “[Appropriate Filtering](http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-for-education-settings)”

[Somerset Guidance for schools – questions for technical support](https://www.somerset.org.uk/sites/edtech/eSafety/Leading/Questions%20for%20Technical%20Support%202018.pdf)  – this checklist is particularly useful where a school uses external providers for its technical support/security.

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed: [SWGfL Test Filtering](http://testfiltering.com/)