## Filtering Policy

| Written by | Victoria Gillies | | ICT Coordinator | |
|---|---|---|---|---|
| Owned by | Name | | Job Title | |
| Applies to | Staff | ☐ | Students | ☐ |
| | Parents | ☐ | Governors | ☐ |
| Reviewed on | November 2014 | | | |
| To be reviewed on | July 2015 | | | |
| Agreed by governors | __/__/____ | | | |

### 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 e-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.

### Key Personnel

*Who will be responsible for creating and reviewing the policy – ICT Coordinator. Miss V Gillies.*
*Who can provide educational and technical expertise on Internet filtering – Technician – Paul Price – MGL.*

### Responsibilities

The responsibility for the implementation of the school's filtering policy will be held by (*Miss V Gillies*). 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** (Mr P Graham)**:**
- *To be reported to a second responsible person every half term in the form of an audit of the change control logs*

- *be reported to the E-Safety Group every half term in the form of an audit of the change control logs*

All users have a responsibility to report immediately to (ICT Coordinator) 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 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.

- Any breach of the filtering policy will result in action in live with the United Learning Disciplinary Policy
- *The academy manages its own filtering service*
- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.*
- *Mobile devices that access the academy internet connection (whether school / academy 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 technical staff. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Group.*

## Education / Training / Awareness

*Pupils / students* will be made aware of the importance of filtering systems through the e-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.*

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

## 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 E-Safety Policy and the Acceptable Use Agreement.

## Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- *the second responsible person*
- *E-Safety Group*
- *E-Safety Governor / Governors committee*
- *External Filtering provider / Local Authority / Police on request*

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