

	<h2>South Bersted CE Primary Filtering Policy</h2>
<b>Web and/or Internal</b>	<b>Web/Internal</b>
<b>This policy should be reviewed every</b>	<b>Three years</b>
<b>Policy approved by Governors</b>	<b>Spring 2023</b>
<b>Date of Review</b>	<b>Spring 2026</b>
<b>Member of staff responsible</b>	<b>Business Manager</b>
<b>Policy created by</b>	<b>SBS Policy</b>
<b>Signed by Chair of Governors and/or Headteacher</b>	

## General Overview of Filtering

To ensure pupils safety whilst retaining the flexibility needed for effective teaching and learning. Filtering of the school's Internet connection cannot guarantee the safety of its pupils and staff, supervision and education are as important as any software solutions.

Filtering is however, a necessary first step to ensure that South Bersted C of E Primary School has taken all reasonable steps to protect pupils and staff. This Policy is to be used in conjunction with the Acceptable Use Policies to provide safe, but productive, access to the Internet.

## Education Content Filtering

Content filtering is an important part of keeping pupils safe, making sure that they don't see inappropriate content online, from adult content to hate speech. With an incredible amount of educational resources available online, pupils now use the Internet far more often, and schools need an effective content filtering solution more than ever before.

South Bersted CE School uses Coconnect Netsweeper Filtering; an online filtering tool that makes sure that pupils are kept safe online while still letting them access useful sites, resources and tools.

Coconnect Netsweeper Filtering is designed to work with Internet connections from Coconnect, using their public IP address and username to determine a profile and apply settings. Providing real-time classification of any accessed site, Cloud enables filtering of any HTTPs site, no matter what device is being used.

With Coconnect Netsweeper Filtering South Bersted C of E Primary School can:

- Completely control filtering, deciding which categories and sites to block, with exception of enforced categories
- Create user and computer groups, and apply different filtering settings to these groups
- Update filtering settings in real time to block or unblock sites as required
- Restrict the use of social media sites
- Restrict the use of sites such as YouTube
- Enforce SafeSearch on internet search engines

Content filtering isn't necessarily a one-size-fits-all matter, particularly in schools. Teachers and pupils often need access to different sites, while different levels of content are appropriate for different age groups. Coconnect Netsweeper filtering enables a range of filtering policies which accommodates for these different profiles and groups

Coconnect Netsweeper Filtering also allows for multiple policies, which can be designated to different groups of users, computers and/or locations, and times as required. Useful websites can be unblocked by authorised teachers to change a site's filtering at any time. Once a change has been made, changes to filtering policies across the school's network activates in real time, so classes have access to approved sites instantly, all changes are fully logged for audit purposes.

Some content will not display at any point. Coconnect Netsweeper Filtering, will keep content like, adverts, hate speech, terrorism or adult material filtered at all times in compliance with KCSIE and Prevent Duty requirements, whilst still letting teachers change filtering for other kinds of content, such as YouTube.

Coconnect Netsweeper Filtering implements a filtering policy across the entire network, filtering content on any connected device. This ensures that pupils and staff are never exposed to inappropriate content, and can get the best possible use out of their tablets / other devices.

Coconnect Netsweeper Filtering includes several enforced categories ranging from filtering violent / adult content to highly filtered walled garden filtering and an option for instantly fulfilling the Prevent Duty's requirements.

In line with the requirements of the 2015 'Keeping Children Safe In Education' guidelines, Coconnect Netsweeper Filtering automatically categorises sites according to their content, enabling websites to be blocked as appropriate, including those containing keywords covering the following content:

- Illegal: content that is illegal, for example child abuse images and terrorist content

- Bullying: Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others
- Child Sexual Exploitation: Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet.
- Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity.
- Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances
- Extremism: promotes terrorism and terrorist ideologies, violence or intolerance
- Pornography: displays sexual acts or explicit images
- Self-Harm: promotes or displays deliberate self-harm
- Violence: Displays or promotes the use of physical force intended to hurt or kill
- Suicide: Suggest the user is considering suicide

Coconnect Netsweeper Filtering also allows multiple filtering policies, enabling different categories for different age groups to be blocked, keeping younger pupils away from more mature content.

## Prevent Duty

Introduced in 2015, the Prevent Duty is a legal requirement that schools protect children from radicalisation, which requires that hate material be filtered. Coconnect Netsweeper filtering includes enforced categories which immediately block certain categories.

These categories immediately block radical material, ensuring the school is in compliance with the duty.

Most large websites don't just have one kind of content, hosting many different kinds of content. Coconnect Netsweeper Filtering assigns multiple classifications to sites which cover different areas, ensuring complete control over how sites with multiple types of content are filtered.

## Malware

Malware embedded in downloaded files is one of the biggest cybersecurity concerns around today. A lot of damaging software, from ransomware to data-stealing programs, is found in files which claim to be something legitimate. Malware spread through this manner is a

major problem for schools, with pupils often having issues when it comes to cybersecurity.

Coconnect Netsweeper Filtering will completely block downloads with certain file name extensions, cutting off the majority of this kind of malware. Stop executable .exe files entirely, block .doc and .ppt files which can contain harmful macros, and more.

Coconnect Netsweeper Filtering logs in real-time how the school's Internet connection is used, providing an overview of how the connection has been used at any time, by any user or device.