Beverley Minster CE Primary School

Online Safety Policy

Date Policy Formally Agreed By Governors:

Date Policy Becomes Effective: October, 2025

Review Date: October, 2027

Person Responsible for Implementation and Monitoring: Head Teacher

1. Introduction and Aims

Keeping children safe in education 2025: Statutory guidance for schools and colleges (Department for Education (DfE, 2025) states that it is essential that children are safeguarded from potentially harmful and inappropriate online material. Online Safety encompasses the use of technology on a wide variety of devices. In school, it can involve the use of online pupil collaboration and publishing and sharing work online. Increasingly, pupil data, work and other information assets are being stored online via learning platforms or other storage facilities.

Outside of school, the availability of online resources is much more wide-spread. The online world develops and changes at great speeds with new opportunities, challenges and risks appearing all the time therefore it is important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. Online safety enables us to provide safeguards and awareness for all users to control and enhance their online experiences. It is not just about the risks and how we avoid them; it is about ensuring everyone has the chance to develop a set of safe and responsible behaviours that will enable them to reduce the risks, whilst continuing to benefit from the opportunities.

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

This policy reflects the school's aims in relation to the teaching and learning of Online Safety. It sets out a framework within which teaching and non-teaching staff can operate. Additionally the policy aims to raise awareness of safety issues associated with electronic communications with all members of our school community.

Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools (June 2019)
- Behaviour in schools Advice for head teachers and school staff (September 2022)
- Meeting digital and technology standards in schools and colleges (updated March, 2023)

This policy also needs to be read in conjunction with the following School policies: Acceptable Use, Strategic Child Protection and Safeguarding Policy, Behaviour Policy, Low-Level Concerns Policy and Whistleblowing Guidance as well as the East Riding of Yorkshire Council policies and guidance for Use of the Internet and Use of Electronic mail (Email).

Our aims for online safety at Beverley Minster Primary school are that:

● there are agreed expectations for the safe and responsible use of digital technologies for learning, administration, and communication

● stakeholders are aware of their responsibilities and understand how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world

● clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms are in place

● children are prepared to be safe and responsible users of online technologies

2. <u>Roles and Responsibilities within Online Safety</u>

Online safety is a safeguarding issue not a computing issue. All members of the school community have a duty to be aware of online safety at all times and to know the required

procedures and to act on them. The following responsibilities demonstrate how each member of the community will contribute.

Governors

Our governors determine, support, monitor and review the school's policies. The governor who has the responsibility for Online Safety will closely monitor this area and regularly meet with the Filtering and Monitoring Leader and where necessary, the Headteacher to discuss developments and progress including, but not limited to:

● the effectiveness of the policy

● current issues in online safety

● reviewing (anonymised) incidents and if possible, filtering and monitoring logs

Head teacher and senior leaders:

● have a duty of care for ensuring the online safety of members of the school community and fostering a culture of safeguarding (though the day-to-day responsibility for online safety may be delegated to the DDSL)

● are responsible for ensuring that the Online Safety Leader, Filtering and Monitoring Leader, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant

● are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff

● ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role

● receive regular monitoring reports from the Filtering and Monitoring Leader

Designated Safeguarding Lead /Deputy Designated Safeguarding Lead (DSL/DDSL):

● will be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from: sharing of personal data, access to illegal/inappropriate materials, inappropriate online contact with adults/strangers, potential or actual incidents of grooming, online bullying.

- will take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- will ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- will liaise with the local authority where necessary

Online Safety Leader:

- will promote an awareness of and commitment to online safety education/awareness both in school and out
- will liaise with the designated safeguarding lead, technical, pastoral and support staff where necessary
- will liaise with subject leaders (particularly of Computing and Personal Development) to ensure that the online safety curriculum is planned, taught, monitored and assessed effectively.

Filtering and Monitoring Leader:

- receive reports of online safety incidents and create a log of incidents on CPOMS to inform future online safety developments
- will provide or identify sources of training and advice for staff and all other members of the school community
- will liaise with the designated safeguarding lead, technical, pastoral and support staff where necessary
- will meet regularly with the online safety governor to discuss current issues, review incidents and filtering and monitoring logs
- will report regularly to the headteacher and the senior leadership team
- will attend and report to, relevant governing board meetings
- will liaise with the local authority where necessary

Teaching and Support Staff:

- will read, understand and implement the Online Safety policy
- will read, understand, agree and adhere to the Acceptable Use policy
- will ensure all online safety incidents are logged in line with this policy
- will maintain a professional level of conduct in personal use of technology and model safe and responsible behaviours in their own usage
- will respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintain an attitude of 'it could happen here'.

Technical Staff (East Riding Local Authority ICT support):

- will read, understand, contribute to and help promote the Online Safety policy
- will read, understand, agree and adhere to the Acceptable Use policy
- will report any Online Safety related issues to the Filtering and Monitoring Leader
- will maintain an awareness of current online safety issues, legislation and guidance relevant to their work and pass any such information to the Filtering and Monitoring Leader
- will maintain a professional level of conduct in the personal use of technology at all times
- will support the school in providing a safe technical infrastructure to support learning and teaching
- will ensure that access to the school network is only through an authorised, restricted mechanism
- will ensure that provision exists for misuse detection and malicious attack
- will take responsibility for the security of the school ICT system and provide regular feedback to the Filtering and Monitoring Leader
- will document all technical procedures and review them for accuracy at appropriate intervals

- will restrict all administrator level accounts appropriately
- will ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- will ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- will ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

Parents:

- will consult with the school if they have any concerns about their children's use of technology
- will help and support the school in promoting online safety
- will take responsibility for their own awareness in relation to the opportunities and risks posed by new and emerging technologies and model safe and responsible behaviours in their own usage
- will discuss online concerns with their children, show an interest in how they are using technology and encourage safe and responsible usage

Visitors, volunteers and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and adhere to it and the Acceptable Use Policy.

3. Procedure for Logging Online Safety Incidents

Any online safety incidents in relation to the categories of risk set out in this policy must be reported immediately to the Head Teacher/DSL/DDSL either face to face where necessary or logged via CPOMS. The log must state which category of risk the incident relates to as well as all other necessary information as any other safeguarding incident (e..g. name/s of child/ren involved, date, time and location of incident). The DSL/DDSL will use the log of information to further investigate the incident and this may involve checking the filtering and monitoring logs, speaking with children and parents.

4. Teaching and Learning

Beverley Minster CE Primary School believes that the key to developing safe and responsible behaviours online, not only for children but everyone within our school community, lies in effective education. We understand that the internet and other technologies are embedded in our children's lives both in school and out and it is our duty to prepare them to be safe online. Children will be taught about online safety as part of the curriculum within, but not limited to Computing and PSHE:

In Key Stage 1, children will be taught to:

- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In Key Stage 2, children will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, children will know:

- that people sometimes behave differently online, including by pretending to be someone they are not
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- how information and data is shared and used online
- what sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- how to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- that for most people the internet is an integral part of life and has many benefits.
- about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- why social media, some computer games and online gaming, for example, are age restricted.
- that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
- how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted.
- where and how to report concerns and get support with issues online.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Parents and Carers

The school will raise parents' awareness of internet safety in letters home, and in information via the school's website and Twitter site. This policy will also be shared with parents. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the

headteacher/DSL and/or the DDSL. A partnership approach will be encouraged with parents which may include practical sessions as well as suggestions for safe internet use at home.

5. **Online child on child abuse**

Online child on child abuse is any form of child on child abuse with a digital element, for example, sexting, online abuse, coercion and exploitation, child on child grooming, threatening language delivered via online means, the distribution of sexualised content and harassment. The Behaviour Policy and Statement of Behaviour Principles outlines Beverley Minster Primary School's procedures for managing these areas of online safety.

Cyber-bullying

Cyber-bullying takes place online, such as through social media sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. The Behaviour Policy outlines procedures for dealing with this specific online safety area.

6. Acceptable Use

All staff, volunteers and governors must sign an Acceptable Use Statement in relation to use of the school's ICT facilities including the internet. Further information is set out in the Acceptable Use Policy.

7. Filtering Internet Access

Beverley Minster Primary School use a filtered internet service provided by ERYC and Smoothwall. The provision includes filtering appropriate to the age and maturity of pupils and we are proactive regarding the nature of content which can be viewed. Beverley Minster Primary School has a clearly defined procedure for reporting breaches of filtering: these are to be logged as incidents on CPOMS and reported directly to the Head Teacher/DSL/DDSL who will then follow these up. If a user discovers a website with inappropriate or potentially illegal content, these are to be immediately reported to a member of staff who will inform the DSL/DDSL. Such incidents will be reported to appropriate agencies including the filtering provider, the local authority, Child Exploitation and Online Protection (CEOP) or the Internet Watch Foundation (IWF). All stakeholders will be aware of these procedures by reading and signing the Acceptable Use Policy.

The following statements apply (*using 'Meeting digital and technology standards in schools and colleges' – updated March, 2023*)

Beverley Minster Primary School will identify and assign roles and responsibilities to manage your filtering and monitoring systems:

The importance of meeting the standard

Schools and colleges should provide a safe environment to learn and work, including when online. 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.

How to meet the standard

The Governing Bodies have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.

To do this, they should identify and assign:

- a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met
- the roles and responsibilities of staff and third parties, for example, external service providers

Technical requirements to meet the standard

The senior leadership team are responsible for:

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

They are also responsible for making sure that all staff:

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

Senior leaders will work closely with governors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will work closely together with ERYC to meet the needs of our setting.

The DSL will take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports

- safeguarding concerns
- checks to filtering and monitoring systems

ERYC has technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

ERYC will work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

Beverley Minster CE Primary School will review filtering and monitoring provision at least annually:

The importance of meeting the standard

For filtering and monitoring to be effective it should meet the needs of our pupils and staff, and reflect our specific use of technology while minimising potential harms.

To understand and evaluate the changing needs and potential risks of our school, we will review our filtering and monitoring provision, at least annually.

Additional checks to filtering and monitoring need to be informed by the review process so that governing bodies have assurance that systems are working effectively and meeting safeguarding obligations.

How to meet the standard

The Governing Body have overall strategic responsibility for meeting this standard. They will make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually.

The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and ERYC - IT service provider and involve the responsible governor. The results of the online safety review will be recorded for reference and made available to those entitled to inspect that information.

Technical requirements to meet the standard

A review of filtering and monitoring should be carried out to identify our current provision, any gaps, and the specific needs of our pupils and staff.

We will audit:

- the risk profile of our pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what our filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of our pupils
- teaching requirements, for example, our RHSE and PSHE curriculum
- the specific use of our chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies we have in place
- what checks are currently taking place and how resulting actions are handled

To make our filtering and monitoring provision effective, our review should inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review should be done as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

There are templates and advice in the reviewing online safety section of Keeping children safe in education.

Checks to our filtering provision need to be completed and recorded as part of your filtering and monitoring review process. How often the checks take place should be based on our context, the risks highlighted in our filtering and monitoring review, and any other risk assessments. Checks should be undertaken from both a safeguarding and IT perspective.

When checking filtering and monitoring systems we will make sure that the system setup has not changed or been deactivated. The checks should include a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

We will keep a log of our checks so they can be reviewed. We will record:

- when the checks took place
- who did the check
- what they tested or checked
- resulting actions

We will make sure that:

- all staff know how to report and record concerns
- filtering and monitoring systems work on new devices and services before releasing them to staff and pupils
- blocklists are reviewed and they can be modified in line with changes to safeguarding risks

Beverley Minster CE Primary School will ensure its filtering systems block harmful and inappropriate content, without unreasonably impacting teaching and learning:

The importance of meeting the standard

An active and well managed filtering system is an important part of providing a safe environment for pupils to learn.

No filtering system can be 100% effective. We need to understand the coverage of our filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet our statutory requirements in Keeping children safe in education (KCSIE) and the Prevent duty.

An effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not:

- unreasonably impact teaching and learning or school administration
- restrict students from learning how to assess and manage risk themselves

How to meet the standard

The Governing Body will support the senior leadership team to procure and set up systems which meet this standard and the risk profile of the school or college.

Management of filtering systems requires the specialist knowledge of both safeguarding and IT staff to be effective. We will ask our provider for system specific training and support where applicable.

Technical requirements to meet the standard

We will make sure our filtering provider is:

- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

Our filtering system will be operational, up to date and applied to all:

- users, including guest accounts
- school owned devices
- devices using the school broadband connection

Our filtering system should:

- filter all internet feeds, including any backup connections
- be age and ability appropriate for the users, and be suitable for educational settings
- handle multilingual web content, images, common misspellings and abbreviations
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provide alerts when any web content has been blocked

Mobile and app content is often presented in a different way to web browser content. Confirmation will be sought from ERYC as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead.

Our filtering systems should us to identify:

- device name or ID, IP address, and where possible, the individual
- the time and date of attempted access
- the search term or content being blocked

Our school will conduct our own data protection impact assessment (DPIA) and review the privacy notices of third party providers. A DPIA template is available from the ICO.

The DfE data protection toolkit includes guidance on privacy notices and DPIAs.

The UK Safer Internet Centre has guidance on establishing appropriate filtering.

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report via CPOMS if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

Beverley Minster Primary School will have effective monitoring strategies that meet the safeguarding needs of the school:

The importance of meeting the standard

Monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software.

Monitoring allows the school to review user activity on school and college devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

Our monitoring strategy will be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

How to meet the standard

The Governing Body will support the senior leadership team to make sure effective device monitoring is in place which meets this standard and the risk profile of the school.

The designated safeguarding lead (DSL) will take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.

The management of technical monitoring systems require the specialist knowledge of both safeguarding and IT staff to be effective. Training should be provided to make sure their knowledge is current. We will ask ERYC for system specific training and support where applicable.

Technical requirements to meet the standard

The Governing Body will support the senior leadership team to review the effectiveness of our monitoring strategies and reporting process. Make sure that incidents are urgently picked up, acted on and outcomes are recorded. Incidents could be of a malicious, technical, or safeguarding nature. It will be clear to all staff how to deal with these incidents and who should lead on any actions.

The UK Safer Internet Centre has guidance for schools and colleges on establishing appropriate monitoring.

Device monitoring can be managed by ERYC, who need to:

- make sure monitoring systems are working as expected

- provide reporting on pupil device activity
- receive safeguarding training including online safety
- record and report safeguarding concerns to the DSL

Make sure that:

- monitoring data is received in a format that our staff can understand
- users are identifiable to the school or college, so concerns can be traced back to an individual, including guest accounts

If mobile or app technologies are used then ERYC will apply a technical monitoring system to the devices, as our filtering system might not pick up mobile or app content.

In the online safety section of Keeping children safe in education there is guidance on the 4 areas of risk that users may experience when online. Our monitoring provision should identify and alert you to behaviours associated with them.

Technical monitoring systems do not stop unsafe activities on a device or online. Staff should:

- provide effective supervision
- take steps to maintain awareness of how devices are being used by pupils
- report any safeguarding concerns to the DSL

School monitoring procedures are reflected in our Acceptable Use Policy and integrated into relevant online safety, safeguarding and organisational policies, such as privacy notices.

Schools and colleges that have a technical monitoring system will need to conduct their own data protection impact assessment (DPIA) and review the privacy notices of third party providers. A DPIA template is available from the ICO.

The DfE data protection toolkit includes guidance on privacy notices and DPIAs.

Additional information in relation to the school's ICT provider (East Riding of Yorkshire Council – ERYC/ER)

Filtering and Monitoring

ERYC are responsible for the firewalls and all blacklisting undesirable URL sites which come under the following categories set by Smoothwall:

Abuse

Adult content

Bullying

Criminal activity

Radicalisation

Substance abuse and

Suicide

No filtering solution can guarantee 100% blacklisting, as unfortunately professional hackers are constantly changing/creating new URLs. Therefore if the school receives any undesirable content, ERYC will work in partnership with the school to manually blacklist this content.

Permissions for access, access restrictions and Safe Search engines

Permissions for access to the internet is controlled by ERYC Firewalls and via ER proxy settings, which gives greater access to Staff and less so for pupils. ER provide these settings to ICT Support providers at each school. ER engineers will ensure the settings are adhered correctly. For example, the pupil settings only allows Education YouTube not the full version access. It is up to the school to decide and review if the full version of Youtube can be used by Staff and Pupils, Safe search is enabled for all search engines as well as https decrypt & inspect, which allows ER to filter search terms from explicit content.

Filtering Trained

ER Comms team and Security Team as well as Paul Foster have been trained directly by Smoothwall and are ER experts in this field, with 3rd line support provided direct by Smoothwall if required. All ER Schools staff attend regular in-house Smoothwall training to ensure they are kept abreast of changes.

The filtering provides reports and notification alerts for any breaches of the categories mentioned earlier. These are daily reports should there be a breach, and if a suicide breach, then the DLS/SLT will receive an instant notification, which as a team we also try to notify the school to bring their attention to the alert. To ensure the right personnel receive the notifications, we do require the schools to inform us of any changes in email addresses of the appropriate DLS/SLT throughout the school year.

Users and Devices

Physical logs for devices that are not able to log into a user account to identify the user are advised to be used by Staff/School to monitor access dates and times. Devices with the correct proxy applied will be filtered according to either Key stage or Staff or network administrators. Devices not using a proxy will be filtered as "Transparent" devices, these devices are placed under the highest restriction of filtering due to the fact that we cannot identify who is using the device. The limitations of this is that some content that needs to be accessed could be blocked due to the higher restrictions.