

HARLOW FIELDS SCHOOL & COLLEGE

Working Together To Succeed



POLICY TITLE: **Safeguarding and Cyber Bullying Policy**


ADOPTED: September 2025

COMMITTEE: Full Governing Body (FGB)

DATE FOR REVIEW: September 2026

AUTHOR: Kathleen M Faherty

POLICY NUMBER: HFP - 28

This policy was updated, to take effect from:	September 2025
School staff were consulted on this document, and it was accepted by the personnel committee on:	N/A
It was ratified by the full governing board on:	17 th September 2025
Signed by Chair of Governors	

Designated Safeguarding Lead (DSL) and Deputy DSLs (DDSLs)

- **DSL:** Megan Hood
- **DDSLs:** Kathleen M Faherty, Josh Chadwick, Rebecca Willers

The DSL is responsible for the overall implementation of this policy. The DDSLs support and act in the absence of the DSL. All safeguarding or cyber bullying concerns must be reported to the DSL or a DDSL without delay.

Introduction

Harlow Fields School and College is committed to safeguarding and promoting the welfare of all pupils. We believe every member of the school community has the right to learn, work, and thrive in a safe, supportive, and respectful environment.

We recognise the importance of technology in the lives of our pupils and staff. While digital platforms offer significant educational and social benefits, they also present risks. This policy outlines how the school prevents, identifies, responds to, and monitors safeguarding issues that arise through or alongside cyber bullying. This policy supports the school's wider Safeguarding and Child Protection Policy and is aligned with relevant national guidance, including Keeping Children Safe in Education (KCSIE 2023).

Aims of the Policy

To ensure:

- Pupils, staff, and parents understand what cyber bullying is and the potential consequences
 - Robust procedures are in place to prevent, report, and respond to cyber bullying incidents
 - Pupils affected by cyber bullying receive appropriate support
 - Safeguarding risks associated with digital communication are managed effectively
-

Definition of Cyber Bullying

Cyber bullying is a form of bullying that takes place through digital technology. It may involve the use of:

- Text messaging or phone calls
- Emails
- Social networking platforms
- Messaging apps
- Online gaming platforms
- Photo/video sharing tools
- Websites or forums

The Department for Education defines cyber bullying as:

“An aggressive, intentional act carried out by a group or individual using electronic forms of contact against a victim who cannot easily defend themselves.”

Cyber bullying can include verbal abuse, threats, intimidation, exclusion, impersonation, harassment, and the sharing of private or harmful content. It may relate to race, religion, gender, sexuality, disability, or other personal characteristics.

What Makes Cyber Bullying Different?

- **24/7 Access:** It can happen at any time, including outside school hours
 - **Wide Audience:** Content can spread rapidly to a large audience
 - **Anonymity:** Perpetrators may hide behind false identities
 - **Unintentional Harm:** Some incidents may result from thoughtlessness rather than malice
 - **Evidential Trail:** Digital messages and posts can be recorded, captured, and shared
-

Preventative Measures

The school takes proactive steps to prevent cyber bullying:

- **DSL oversight:** The DSL monitors safeguarding practices, including online safety
 - **Technology systems:**
 - A **Firewall** is provided and maintained by **RM and Schools Broadband**
 - **Senso safeguarding software** is used for real-time monitoring, with weekly reports sent to the DSL
 - Both RM and Schools Broadband comply with **KCSIE 2023** and are members of the **Internet Watch Foundation (IWF)**
 - **Curriculum education:** Pupils are taught about online safety and responsible use of technology through **ICT, PSHE, assemblies**, and enrichment programmes like **Crucial Crew**
 - **Staff training:** Staff are trained in online safety and safeguarding procedures
 - **Reporting culture:** Pupils are encouraged to report concerns through trusted adults and the School Council
-

Reporting Concerns

All safeguarding or cyber bullying concerns must be reported **verbally and immediately** to a member of the **Safeguarding Team (DSL or DDSLs)** to ensure prompt action.

Following the verbal report:

- The concern **must be recorded without delay** on **RecordMy** by the staff member who received the information
 - The DSL or DDSL will oversee the situation and ensure all necessary **follow-up actions** are completed promptly and appropriately
 - Pupils, staff, and parents are encouraged to report concerns and know that doing so helps keep everyone safe
 - Information about external support services (e.g., **Childline**) is shared with pupils and parents
-

Responding to Incidents

Each case will be assessed and responded to based on the needs of those involved and the nature of the incident.

The response may include:

- Offering emotional support to the victim
 - Preserving evidence (e.g., messages, screenshots)
 - Investigating the situation using digital safety logs, pupil/staff statements, and Senso alerts
 - Involving parents/carers of all parties
 - Considering disciplinary action for perpetrators in line with the **Behaviour Policy**
 - Referring serious cases to external agencies (Police, Children's Social Care)
 - Reviewing online safety education and pastoral support
-

Sanctions and Support

Sanctions are used to:

- Protect the victim and stop further abuse
- Ensure the perpetrator understands the harm caused
- Prevent repeat incidents
- Demonstrate to the school community that cyber bullying is taken seriously

Support may also be offered to the perpetrator, particularly where issues such as peer pressure, lack of digital understanding, or SEND are contributing factors. External agencies (e.g., **Children with Disabilities Team, Police**) may be involved where necessary.

Monitoring and Evaluation

- **The DSL** will report on safeguarding and cyber bullying trends to the **Governing Body** via termly safeguarding reports
 - **The Governing Body** is responsible for reviewing and approving this policy annually
 - The school will evaluate the effectiveness of its prevention and response measures and make updates as required
-

Appendices

- **Appendix 1:** Guidance for Parents and Pupils
 - **Appendix 2:** Examples of Technologies and Misuse
 - **Appendix 3:** Staff Roles and Professional Responsibilities in Online Safety
-

Key Contacts

Designated Safeguarding Lead (DSL):

- Megan Hood

Deputy Designated Safeguarding Leads (DDSLs):

- Kathleen M Faherty
- Josh Chadwick
- Rebecca Willers

Appendix A

Interm IT - Partnership Document with Harlow Fields School and College

Digital and Technology standards in schools and colleges March 2023

In this document we clarify the key responsibilities that fall to governing bodies and leadership teams under the March 23 guidance from the Dfe and identify the support and expertise that Interm IT provides for our schools as we work together to ensure the safeguarding of young people. We ask that you complete or correct any school information and ensure that the relevant staff and governors have sight of the completed document which should be available for inspection when required.

All governing bodies and leadership teams should be fully aware of, and be putting into practice, the statutory guidance in KCSIE 22/23; appreciating the role of all parties in ensuring online safety is firmly embedded as a safeguarding issue.

The March 23 guidance from the Dfe offers more clarity around roles and responsibilities in relation to digital and technology standards in schools and in particular to filtering and monitoring. This area is likely to come under significant scrutiny in Ofsted inspections going forward.

The guidance identifies 4 filtering and monitoring standards:

Standard 1

You should identify and assign roles and responsibilities to manage your filtering and monitoring systems.

Governing bodies have overall strategic responsibility for filtering and monitoring and need to be assured that these standards are being met. Schools should identify and assign a member of the school leadership team and a governor to be responsible for ensuring these standards are met. There must be clarity over the roles and responsibilities of staff and third-party providers including Interm IT.

The assigned member of the school's senior team is Megan Hood.

They will fulfill their responsibility by ensuring that

e.g. report Half termly to the governing body, lead item on inset day, staff meetings, check that filtering and monitoring is working

The nominated governor is Sarah Dodd. They will ensure that the standards are being met and will report to the governing body termly.

Governor understands how it is done and that it is working.

Standard 2

You should review your filtering and monitoring provision at least annually

As part of their routine annual appointment to review the contract with each school Interm IT will, working with the school, ensure that the documentation that the school holds regarding its filtering and monitoring systems is both accurate and technically sound. Interm IT will use their technical expertise, and their knowledge of industry trends and technological advances, to advise school leaders on whether their provision remains best value and whether within the financial restraints of the school, it still delivers best practice in this area - thus enabling the school to justify its procurement decisions. Any change to the system set up will have an impact on the decisions made, for example the use of school owned devices off site, and the impact of this will be reflected on during the review. In addition, a discussion around roles and responsibilities is essential at least annually to ensure that Interm's staff are working effectively with the school staff so that there can be no slippage in either filtering or monitoring. The results of the annual review must be retained by the school and be available for inspection.

Our annual review takes place in the Autumn term.

The school staff attending will be Kathleen (Head) and / or Megan Hood (DSL)

Standard 3

Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning

Again, as part of the annual meeting Interm will advise the school on how to ensure that filtering does not impact teaching and learning whilst at the same time enables the school to meet its statutory requirements in KCSIE and Prevent duty. Schools must give thought as to how to enable students to assess and manage risk themselves. The Interm staff on site will also be able to provide real time support in this area as the need arises throughout the school year.

The school filtering system is hosted by RM (school) and Talk Straight (6th form) and utilises the following RM Safetynet and Netsweeper software respectively.

Standard 4

You should have effective monitoring strategies that meet the safeguarding needs of your school.

Monitoring user activity on school devices is an essential part of providing a safe environment for students and staff. Unlike filtering, it does not stop users from accessing material, but it allows the school to review user activity on school devices. For monitoring to be effective it must pick up incidents urgently, allowing prompt action to be taken and outcomes to be recorded.

Again, a clear staff responsibility structure is key as are delineated procedures. The specialist knowledge of both safeguarding and IT staff is required to enable the management of technical monitoring systems.

Interm partner with a market leader provider of effective monitoring software but we can work with any provider chosen by the school. We will be able to ensure that the key staff have appropriate training and given our experience across a range of schools we will guide and advise on good practice in this area.

The monitoring software used is Senso.

The alerts are directed to the DSL from Senso; in their absence the alerts will be sent to Head@