‘Growing together in the spirit of Christ’s love’

All Hallows Catholic High School

Online Safety Policy

Signed by:

Headteacher: Mrs A Cooper

Chair of Governors: Mrs L Kitto

Date: Autumn Term 2025

Review Date: Autumn 2026

Contents

8. **Acceptable Use Policies and Device Usage**
    - Staff and Pupil AUPs
    - Device Usage (School Devices, Personal Devices, Wearable Technology)
    - Monitoring and Privacy
    - Training and Support
9. **Digital Images and Video**
    - Consent and Usage
    - Guidelines for Staff
    - Pupil Education
    - Parental Responsibility
10. **Trips, Events, and Personal Device Usage**

- School Trips and Events
- Device Usage in School (Pupils and Staff)
- Visitor Device Policy
- Parent Guidelines for Events

11. **Searching and Confiscation**

- Authority to Search
- Confiscation of Devices
- Managing Sensitive Content
- Parental Involvement

12. **Appendix – Roles and Responsibilities Summary**

- Headteacher
- Designated Safeguarding Lead (DSL)
- Governing Body
- Staff
- Technical Staff
- Pupils
- Parents
- Data Protection Officer (DPO)

Introduction and Key Changes for 2025

This policy reflects essential updates for September 2025, aligning with new standards in online safety and digital safeguarding as mandated by "Keeping Children Safe in Education" (KCSIE) 2024. The Designated Safeguarding Lead (DSL) now holds primary responsibility for web filtering and monitoring, requiring close collaboration between technical and safeguarding teams.

Schools must adopt robust filtering and monitoring strategies to ensure compliance, focusing on balancing security with accessible learning resources. This document outlines the specific responsibilities of all school stakeholders, including staff, governors, and technical support, in maintaining a safe digital environment.

Purpose of the Policy This Online Safety Policy provides a framework for safeguarding in digital spaces across the entire school community. It aims to:

- Establish standards for online behaviour for staff, pupils, and all stakeholders.
- Define roles in digital safety management, from DSLs to governors.
- Support compliance with KCSIE and RSHE requirements for digital resilience.

Roles and Responsibilities

1. **Designated Safeguarding Lead (DSL) & Whole School ICT Lead**
    - Leads online safety and digital safeguarding efforts, ensuring regular monitoring and annual reviews of filtering and monitoring systems.
    - Delegates tasks as appropriate but retains overall responsibility for implementing online safety policies.
    - Coordinates with technical teams to review the effectiveness of current systems and conducts staff training on latest updates and standards.
    - Provides guidance to all school staff on handling online incidents and maintaining compliance with safeguarding practices.
2. **Governors**
    - Ensure that online safety policies are comprehensive, updated, and effectively implemented.
    - Work closely with the DSL and IT personnel to oversee filtering and monitoring measures.
    - Participate in regular training on online safety standards to stay informed of best practices.
    - Support school leadership in promoting a culture of digital safeguarding within the school.
3. **All Staff**
    - Comply with the Acceptable Use Policy (AUP) and model appropriate online behaviour.
    - Report any online safety incidents to the DSL promptly.
    - Integrate online safety practices into the curriculum where applicable and reinforce positive digital habits among pupils.

4. **Technical Staff**
    - Support DSL by implementing, maintaining, and reviewing filtering and monitoring systems.
    - Ensure that network security, data protection, and internet safety protocols are up to date.
    - Communicate potential vulnerabilities or incidents to the DSL and perform routine checks to maintain the school's online security infrastructure.
5. **Pupils and Parents**
    - Pupils are expected to understand and adhere to the school's online safety guidelines and report concerns to staff.
    - Parents are encouraged to monitor their children's internet use at home and cooperate with school initiatives to reinforce safe online practices.

Education and Curriculum

The school integrates online safety within the curriculum to equip students with the skills and knowledge for safe digital navigation. Key elements include:

1. **Embedding Online Safety in Curriculum**
    - Online safety concepts are introduced through subjects like PSHE, Computing, and RSHE, covering responsible online behaviour, privacy, and security.
    - The school follows guidance from the DfE: "Teaching Online Safety in Schools," using a whole-school approach to address digital resilience.
2. **Age-Appropriate Content**
    - Curriculum content is carefully sequenced and tailored to each stage of student development, ensuring age-appropriate learning.
    - Online safety education spans topics like self-image, managing online relationships, managing online bullying, and understanding digital reputation.
3. **Supporting Vulnerable Pupils**
    - Additional support and interventions are provided for pupils identified as vulnerable or at higher risk online.
    - Teachers and staff assess understanding through assignments or self-evaluations to capture progress and identify areas needing reinforcement.
4. **Parental Involvement**
    - Parents are encouraged to participate in online safety discussions with children, and resources are provided to aid understanding of current risks and responsible practices.

The school aims to foster digital resilience by preparing students to manage the challenges and risks they may encounter online, both in school and beyond.

Managing Safeguarding Concerns and Incidents

The school treats online safety as an integral part of its safeguarding strategy. Any concerns related to online safety are addressed with the same seriousness as other safeguarding issues, following established protocols:

1. **Reporting and Response**
    - Staff must report any online safety concerns immediately to the DSL, who is responsible for assessing the situation and determining next steps.
    - Urgent issues are addressed within the same day, with the DSL coordinating necessary support or referral to external agencies, if required.
2. **Incident Management for Pupils**
    - Pupils are encouraged to report issues they encounter online, with clear guidance on how to seek help.
    - Parents are informed of incidents involving their children where appropriate, and support resources are provided to help families address online safety at home.
3. **Special Cases: Sexting, Upskirting, and Bullying**
    - **Sexting**: The school follows UK Council for Internet Safety (UKCIS) guidelines to manage cases of sharing nudes or semi-nudes. Staff are instructed not to view, share, or delete any images but to refer the matter to the DSL immediately.
    - **Upskirting**: Recognised as a form of sexual harassment, upskirting is handled with sensitivity and care, following legal and safeguarding protocols.
    - **Bullying**: Online bullying incidents are addressed in alignment with the school's anti-bullying policy, with measures in place to provide support to affected pupils and promote a respectful online environment.
4. **External Agency Support**
    - The school may engage with external agencies (e.g., Police, NSPCC) when incidents are severe or criminal, ensuring pupil safety and well-being remain the priority.

By implementing clear procedures and prioritising swift action, the school aims to provide a safe environment for pupils in both physical and online spaces.

Filtering and Monitoring

In alignment with the Department for Education (DfE) standards, the school utilises appropriate filtering and monitoring systems to safeguard pupils while allowing educational access to online resources:

1. **Filtering Standards**
    - The school's filtering system, managed by the DSL and IT staff, blocks harmful and inappropriate content without disrupting access to necessary educational materials.
    - Regular checks are conducted to ensure filtering settings remain effective, with logs maintained for accountability.
2. **Monitoring Systems**
    - The school employs a variety of monitoring strategies, including live supervision, network logs, and individual device checks, to track digital activity and detect potential risks.
    - Staff are trained to recognise and report any unusual online behaviour, ensuring any gaps in filtering are addressed.
3. **Roles and Responsibilities**
    - The DSL and person responsible for whole school ICT oversees filtering and monitoring with support from technical staff, who implement necessary adjustments and conduct regular audits.
    - All staff members play a role in identifying over blocking or bypassing issues and providing feedback to help maintain balanced filtering.
4. **Balancing Access and Safety**
    - The school aims to avoid excessive restrictions while maintaining online safety standards, fostering a productive digital learning environment.
    - Filtering and monitoring policies are reviewed annually to adapt to new risks and technologies.

These measures provide a layered approach to digital security, prioritising a safe online environment that supports learning and well-being.

Social Media and Digital Presence

The school recognises the importance of managing its online reputation and guiding students, staff, and parents in responsible social media use. The following protocols help maintain a positive and secure digital presence:

1. **School's Social Media Accounts**
    - The school actively monitors its official social media accounts and engages with the community responsibly to maintain a positive online image.
    - The Headteacher oversees account management and responds to any concerns raised about the school on digital platforms.
2. **Guidance for Staff**
    - Staff are expected to maintain high standards of professionalism on personal and school-related social media accounts.
    - They are advised not to connect with pupils on personal accounts and to use strict privacy settings to protect personal content.
    - Staff should avoid posting school-related matters on personal accounts and should refer concerns to appropriate school channels.
3. **Pupil and Parent Conduct**
    - Pupils are discouraged from interacting with staff on social media and are taught safe practices, including the importance of privacy and respectful online conduct.
    - Parents are encouraged to address any school-related issues privately rather than on public platforms and to support the school's social media guidelines.
    - The Acceptable Use Policies (AUPs) outline expected behaviour and potential consequences for breaches.
4. **Training and Resources**
    - The school provides resources to educate the community on safe social media practices and digital footprint management.
    - Regular reminders are issued about online reputation management, and any changes in social media policies are communicated to all stakeholders.

These guidelines help ensure that social media is used constructively and that interactions reflect the school's values and commitment to a safe online environment.

Data Protection and Cybersecurity

The school is committed to protecting personal information and ensuring that all digital activities comply with data protection and cybersecurity standards. Key protocols include:

1. **Data Protection Compliance**
    - All staff, pupils, and contractors are bound by the school's Data Protection Policy, which aligns with the Data Protection Act 2018 and UK GDPR.
    - Sharing information for safeguarding purposes is prioritised; staff are trained to manage data responsibly without unnecessary consent requirements when safety is at stake.
2. **Cybersecurity Measures**
    - The school employs robust security measures, including encryption, password protection, and access controls, to prevent unauthorised access to data.
    - Regular audits and updates are conducted to address emerging security threats and ensure compliance with DfE cybersecurity standards.
3. **Managing Sensitive Information**
    - Staff are reminded of the importance of maintaining confidentiality and storing data securely. Retention schedules are adhered to, ensuring that safeguarding records are preserved as required.
    - Access to sensitive data is limited to authorised personnel, with logs and audits maintained to monitor compliance.
4. **Incident Response and Reporting**
    - In the event of a data breach or cybersecurity incident, staff must report it immediately to the Data Protection Officer (DPO) or DSL.
    - The DPO oversees investigations, coordinates with relevant authorities, and ensures affected parties are informed, as necessary.

Through these practices, the school aims to protect sensitive information, comply with legal standards, and create a secure digital environment.

Acceptable Use Policies and Device Usage

The Acceptable Use Policies (AUPs) establish clear guidelines for the responsible use of school devices and networks, ensuring a safe and productive digital environment for all.

1. **Staff and Pupil AUPs**
    - All staff and pupils must read and sign the AUPs, agreeing to uphold standards of appropriate behaviour when using school devices and networks.
    - AUPs outline prohibited activities, such as accessing inappropriate content, cyberbullying, and unauthorised sharing of information.
    - Any violation of AUPs may result in disciplinary action in line with the school's behaviour policies.
2. **Device Usage**
    - **School Devices**: Staff and pupils must use school-provided devices for educational purposes and follow data protection guidelines. Misuse of devices, whether on-site or remotely, may result in restricted access.
    - **Personal Devices (BYOD)**: Pupils and staff may bring personal devices only for emergency use or as authorised by the school.
    - **Wearable Technology**: Personal wearable devices are not permitted to access school networks and must remain off in restricted areas.
3. **Monitoring and Privacy**
    - The school reserves the right to monitor device usage, email communications, and internet access on school devices to ensure compliance with AUPs.
    - Staff and pupils are reminded that while reasonable privacy is respected, all school-provided systems are monitored for security and policy adherence.
4. **Training and Support**
    - Training sessions are provided for all users to understand the AUPs and expectations surrounding digital conduct.
    - Any changes to device usage policies are communicated through training and policy updates to keep stakeholders informed.

By establishing clear AUPs, the school promotes a responsible digital culture, reinforcing safe and respectful technology use.

Digital Images and Video

The school has policies in place regarding the use of digital images and videos to protect the privacy and safety of pupils and staff. Key points include:

1. **Consent and Usage**
    - Upon joining, parents and guardians provide consent for their children's images to be used in various school-related contexts, such as displays, newsletters, and the school website.
    - Staff must check consent records before using pupil images in public-facing materials. Images used for educational or promotional purposes are kept within the scope of the original consent provided.
2. **Guidelines for Staff**
    - Staff may use school devices to capture images and videos for educational purposes only. Personal devices are generally prohibited for this use to maintain data protection standards.
    - Images taken must be stored on secure school systems and deleted from devices after use, following data retention policies.
3. **Pupil Education**
    - Pupils are taught about privacy, including the importance of not sharing images of others without permission.
    - Lessons include discussions on digital footprint, privacy settings, and the potential risks of sharing personal images online.
4. **Parental Responsibility**
    - Parents attending school events are asked to be mindful of privacy considerations, avoiding the capture or sharing of images featuring other children without permission.
    - The school provides guidance on appropriate image sharing to help maintain a respectful community environment.

These guidelines aim to protect individuals' privacy while allowing the school to celebrate achievements and share activities responsibly.

Trips, Events, and Personal Device Usage

Specific guidelines govern the use of personal and school devices during school trips, events, and in daily school settings to maintain a secure and respectful environment:

1. **School Trips and Events**
    - Staff are provided with school-duty phones for communication during off-site trips to avoid sharing personal contact information.
    - Pupils are allowed limited use of personal devices on school trips for emergencies or educational activities, with prior approval and under staff supervision.
2. **Device Usage in School**
    - **Pupils**: Personal devices, including mobile phones, are permitted in school only for emergency use and must remain off during lessons unless authorised by a teacher for learning purposes. Misuse of devices can result in sanctions, including the temporary withdrawal of privileges.
    - **Staff**: Staff are expected to use personal devices in private staff areas only, ensuring they do not interfere with their duties or pupil supervision. Mobile phone use in the presence of pupils is restricted to emergency situations.
3. **Visitor Device Policy**
    - Visitors, including contractors and volunteers, are requested to keep devices turned off in school premises and are not permitted to take photos or videos of pupils unless authorised by the headteacher.
4. **Parent Guidelines for Events**
    - During school events, parents are asked to seek permission before taking photos or videos that include other pupils and to avoid sharing such content publicly without consent.
    - The school provides reminders on privacy expectations at events to foster a respectful community environment.

These protocols help balance the convenience of personal devices with the need to maintain privacy, safety, and focus in school and during school-related activities.

Searching and Confiscation

The school has established procedures for searching pupils and confiscating items, including electronic devices, to maintain safety and discipline in line with the Department for Education's guidance:

1. **Authority to Search**
    - The Headteacher and authorised staff have the legal authority to search pupils and their belongings if there is reasonable suspicion of prohibited items, including electronic devices containing inappropriate material.
    - Searches are conducted respectfully, in the presence of another staff member, and with consideration for pupils' rights and privacy.
2. **Confiscation of Devices**
    - If a pupil's device is suspected of containing inappropriate or harmful content, staff may confiscate the device temporarily for review by the DSL or a designated staff member.
    - Confiscated items are held securely and returned to the pupil or parent following a review. In cases involving serious concerns, external authorities (e.g., the police) may be consulted.
3. **Managing Sensitive Content**
    - Staff are trained to avoid viewing explicit content and to report any concerning materials to the DSL, who will assess and take appropriate action.
    - In incidents involving potentially illegal content, such as explicit images, staff are advised to follow safeguarding procedures without compromising the evidence.
4. **Parental Involvement**
    - Parents are informed of searches involving their child's device and the reasons behind it, unless doing so would compromise the investigation.
    - The school promotes an open dialogue with parents about device use, privacy expectations, and the importance of adhering to school policies.

These procedures ensure that searches and confiscations are conducted professionally and align with safeguarding standards.

Appendix – Roles and Responsibilities Summary

This appendix provides an overview of key responsibilities for each role in supporting online safety and safeguarding across the school community:

1. **Headteacher**
    - Fosters a culture of safeguarding where online safety is integral to all practices.
    - Oversees the DSL's activities, ensuring compliance with safeguarding policies and online safety protocols.
    - Ensures all staff and governors receive regular training on safeguarding, including online safety.
2. **Designated Safeguarding Lead (DSL) & Whole School ICT Lead**
    - Leads and coordinates online safety and safeguarding efforts, including filtering and monitoring.
    - Maintains updated training, policies, and incident logs, reporting to governors and senior leadership.
    - Supports staff and pupils in understanding online risks and appropriate responses.
3. **Governing Body**
    - Provides strategic oversight of online safety policies, approving updates and reviewing their effectiveness.
    - Participates in training on safeguarding and online safety to stay informed of best practices.
    - Works with the DSL and Headteacher to promote a safe and respectful digital environment.
4. **Staff**
    - Models safe and responsible online behaviour, following AUP guidelines.
    - Identifies and reports online safety incidents to the DSL.
    - Integrates online safety practices into teaching and supports pupils in developing digital resilience.
5. **Technical Staff**
    - Implements and maintains filtering and monitoring systems, coordinating with the DSL for regular reviews.
    - Ensures network security and compliance with data protection standards.
    - Assists in training staff on cybersecurity measures and the appropriate use of technology.
6. **Pupils**
    - Abides by the AUP, reporting concerns about online safety and seeking help when needed.
    - Participates in online safety education and develops responsible digital habits.
7. **Parents**

- Supports school policies on online safety, reinforcing safe practices at home.
- Monitors their child's use of technology and engages in open discussions about online behaviour.

8. **Data Protection Officer (DPO)**
    - Ensures data protection policies are up to date and aligned with safeguarding standards.
    - Manages data breaches responsibly and ensures compliance with GDPR.