NOTRE DAME HIGH SCHOOL

ON-LINE SAFETY POLICY

"If you have love for one another, then everyone will know that you are my disciples"

(John 13:35 GNB)

Online Safety and Safeguarding Policy

1. Purpose of the Policy

The purpose of this policy is to:

- Ensure the safety and wellbeing of children, young people, and adults when using the internet, social media, or mobile devices.
- Provide staff and volunteers with clear and concise guidance on online safety principles and practices.
- Ensure that the school operates in line with its values and complies with the law in how we use and manage online devices.

This policy applies to all staff, volunteers, students, and anyone involved in activities associated with **Notre Dame High School**.

2. Legal Framework

This policy is based on key legislation, policy, and guidance designed to protect children in England. Summaries of the relevant legislation and guidance are available from the following sources:

- Online abuse: NSPCC Online Abuse
- Bullying: NSPCC Bullying
- Child protection system: NSPCC Child Protection

We believe that:

- Children and young people should never experience abuse of any kind.
- Children should be able to use the internet for education and personal development, but safeguards must be in place to ensure they are kept safe at all times.

We recognise that:

- The online world provides many opportunities but also presents risks and challenges.
- It is our duty to protect all children, young people, and adults within the organisation from potential harm online.
- We have a responsibility to keep children and young people safe online, whether they are using the school's network and devices or not.
- All children, regardless of their background, have the right to equal protection from harm or abuse.
- Working in partnership with children, young people, their parents, carers, and other agencies is essential in promoting online safety.

---

3. Online Safety Practices

To protect children and young people, we will:

- Appoint a dedicated **Online Safety Coordinator** to oversee online safety matters within the school. (This is the Designated Safeguarding Lead)
- Provide clear guidance to staff and volunteers on appropriate online behaviour through the **Staff Code of Conduct**.
- Support and encourage students to use the internet, social media, and mobile phones safely and respectfully.
- Develop an **Acceptable Use Agreement** for students and their parents/carers.
- Encourage parents and carers to actively engage in keeping their children safe online.
- Establish clear and effective procedures for responding to incidents of inappropriate online behaviour.
- Review and update the security of our information systems regularly.
- Ensure that usernames, passwords, and other log-in information are securely managed.
- Ensure personal information is held securely and shared only when appropriate.
- Ensure that images of students are used only with written consent and for the purpose agreed upon by the individual and their parent/carer.
- Provide regular supervision, support, and training for staff and volunteers regarding online safety.
- Assess new technologies and social media platforms before their use in the school.
- Implement appropriate filtering and monitoring systems for all IT devices, ensuring real-time alerts are generated to flag concerning online activities (e.g., self-harm, radicalisation).

---

4. Filtering and Monitoring System

As part of our online safety measures, we use the **Sophos Filtering and Monitoring System**, which allows for the real-time detection of inappropriate online activity across school IT systems. This system flags searches, websites, and content that may pose a risk to students, staff, or visitors.

- **Real-Time Alerts and Response**: Alerts are immediately received by the **Designated Safeguarding Lead (DSL)**, who will take action based on the nature of the concern:
    - **Inappropriate content**: The DSL may contact a member of the pastoral or safeguarding team to investigate further or log the issue as an online safety concern in **CPOMS** (Child Protection Online Management System).
    - **Self-harm or Suicidal Ideation**: These alerts require **immediate contact with home** to inform parents/guardians. In cases of unavailability of the DSL, the **Deputy DSL** will also receive these alerts.
    - **Radicalisation**: Alerts indicating extremist or radicalisation-related content will be managed according to the school's safeguarding procedures, including contact with home and referral to appropriate authorities.
    - **Student Safety**: Any alerts related to student safety will be investigated promptly by the DSL, safeguarding team, and where necessary, external authorities.
- **Weekly Reports and Monitoring**: Weekly reports generated by the monitoring system will be reviewed by the DSL to assess risk patterns, identify potential issues, and inform ongoing IT risk assessments. These reports help to ensure our systems are effective and up-to-date in detecting potential risks.

- Where a Fastvue report or alert is received for a site where the data transfer is less than 1000 bytes (1Kb) then no further action is required as this is not sufficient data to have displayed anything on the user screen. Alerts of this type are logged by Fastvue when a website is blocked and the block message (usually less than 1000 bytes but can be up to 1.5K) is displayed or where it is blocked invisibly to the user (0 bytes) This is often the case where an alert is triggered by popups advertising on legitimate sites – eg Gambling sites advertising on a news site.

- There is some discretion required – if the same user hits many blocked sites in a short space of time this may be an attempt to access that kind of site so even though all the attempts are blocked and or the data transfer is small this would need looking at.

---

5. Responding to Online Abuse

In the event of online abuse, we will take the following steps:

- **Clear Safeguarding Procedures**: We have established robust procedures for dealing with online abuse, whether involving staff, students, or external individuals.
- **Staff Training**: All staff and volunteers will be trained to recognize and respond to various forms of abuse, including cyberbullying, emotional abuse, sexting, sexual exploitation, and online harassment.
- **Tailored Support**: Our response will consider the needs of the individual experiencing the abuse, any bystanders, and the wider organisation.
- **Ongoing Review**: The effectiveness of our approach to online abuse will be regularly reviewed and updated.

---

6. Roles and Responsibilities

- **DSL (Designated Safeguarding Lead)**: The DSL is responsible for overseeing online safety within the school. They handle concerns, liaise with parents and authorities, and ensure appropriate action is taken when incidents arise.
- **Deputy DSL**: In the absence of the DSL, the Deputy DSL assumes responsibility for safeguarding, including responding to real-time alerts related to self-harm or student safety.
- **Pastoral/Safeguarding Team**: This team works closely with the DSL to manage concerns, provide support, and investigate potential safeguarding issues.
- **Staff**: All staff members are required to adhere to safeguarding procedures and report any concerns regarding online safety to the DSL.

---

7. Related Policies and Procedures

This Online Safety and Safeguarding Policy should be read alongside the following related policies:

- **Child Protection and Safeguarding Policy** (including KCSIE 2025)
- **Managing Allegations Against Staff and Volunteers**
- **Code of Conduct for Staff and Volunteers**
- **Behaviour and Anti-Bullying Policy**
- **Pupil Images Policy**
- **Student Social Media Policy**

- **Student Acceptable Use Agreement**
- **Electronic Devices – Staff Policy**
- **Equality Duty Act**

---

8. Review and Update

- **Review Date**: September 2025
- **Next Review**: September 2026
- **Review Mechanism**: Governors
- **Policy Update**: As required to ensure ongoing compliance with safeguarding and online safety best practices.

Summary

This policy outlines our commitment to protecting children and young people online. Through clear procedures, the use of real-time monitoring systems, staff training, and strong partnerships with parents and carers, we strive to provide a safe digital environment for all students and staff at Notre Dame High School