Online Safety Policy

From Staff Policies

Policy Details
Legal Status
Non Statutory
Adopted
February 2018
Version Date
February 2018
Last Review
February 2019
Next Review
February 2020
Responsible SMT
NH

Contents

Relevant legislation

Children Act (2004) (http://www.legislation.gov.uk/ukpga/2004/31/contents)

Computer Misuse Act (1990) (http://www.legislation.gov.uk/ukpga/1990/18/contents)

Malicious Communications Act (1988) (http://www.legislation.gov.uk/ukpga/1988/27/contents)

Police & Justice Act (2006) (http://www.legislation.gov.uk/ukpga/2006/48/contents)

Purpose

To safeguard and protect all members of the school community online, identifying approaches to educate and raise awareness of online safety throughout the community. All staff should work safely and responsibly, role model positive behaviour online and manage professional standards and practice when using technology.

The school identifies that the issues classified within online safety can be broadly categorised into three areas of risk :

- **Content** : being exposed to illegal, inappropriate or harmful material
- **Contact** : being subjected to harmful online interaction with other users
- **Conduct** : personal online behaviour that increases the likelihood of, or causes, harm

Principles

The school believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online. It identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life, and that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

The school will ensure that online safety is treated as a safeguarding issue (rather than a technical issue) and as a partnership concern, not limited to school premises, equipment or hours.

Detail

Incidents will be reported via CPOMS (https://priorylewes.cpoms.net/auth/identity?origin=https://priorylewes.cpoms.net/) . A comprehensive range of resources will be provided to parents and carers via the school website (https://www.priory.e-sussex.sch.uk/516/online-safety) . All staff will undertake appropriate CPD such as the SSS E-Safety course (https://training.ssscpd.co.uk/) . Online safety will be addressed in both the Life Skills and Computing curriculums, and worldwide initiatives such as Safer Internet Day (https://www.saferinternet.org.uk/safer-internet-day/) will be actively promoted in school. Industry-standard filtering and logging, meeting DfE requirements, will be used on the school's internet connection. An online safety working group including parental and student representatives will meet regularly to review best practice.

The following is a list of specific **procedures** relating to online safety. As new technologies come into use, best practice may change rapidly and therefore these operational documents may be updated as circumstances require, within the principles of this policy but without the need for further consultation.

- Internet Access Protocol for ICT Technicians
- Internet Filtering Protocol
- Internet Filtering Provider Response
- Online Safety Incidents Procedure
- Personal Devices Rules for Students
- Personal Devices Guidance for Visitors
- Social Media Protocol
- Twitter Protocol

Roles and Responsibilities

The **Governing Body** is responsible for reviewing the policy annually

The **Designated Safeguarding Lead**

- has overall responsibility for online safety as per Keeping Children Safe In Education (2018) (https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)

The **Information Manager**

- is the designated E-Safety Officer, who leads the ICT team to provide technical advice and monitor network activity

Staff and other authorised users (e.g. PGCE students, Governors, EWO)

- must follow the procedures detailed above

Staff, **Student** and other authorised users

- must sign and follow the AUP – Staff, AUP - Student, AUP - Visitors or AUP - Cloud as appropriate
- must follow the AUP – External Services if using external services such as remote access
- must sign and follow the AUP (BYOD) - Staff or AUP (BYOD) - Visitors as appropriate if using BYOD (Bring Your Own Device)

Parents and carers

- must follow the AUP – External Services if using external services such as remote access

Failure to follow the procedures or Acceptable Use Policies (AUPs) referred to above may lead to sanctions, disciplinary action or the involvement of the police or local authority.

Monitoring and Evaluation

Technology in this area evolves and changes rapidly. This policy will be revised following any national or local policy requirements, any child protection concerns or any major changes to the technical infrastructure. It will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments made to the relevant legislation. The Governing Body will monitor the effectiveness of the policy through its Strategic Organisation Committee, and review it as part of their cycle of Policy Review.

Related Documents and Locations

AUP - Student (Supplementary Agreement)
Discovery of Inappropriate Material - Guidance for ICT Technicians
E-Safety Advice To Students
Electronic Imagery and Online Safety
Keeping Children Safe In Education (2018) (https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)
Sexting in schools and colleges: responding to incidents and safeguarding young people (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf)

Related Procedures

- Internet Access Protocol for ICT Technicians
- Internet Filtering

Related Policies

- Anti-Bullying Policy
- Child Protection Policy
- Data Protection Policy
- Network Security Policy
- Student Behaviour Policy

- This page was last modified on 3 May 2019, at 08:08.

Protocol
- Online Safety Incidents Procedure
- Personal Devices Rules for Students
- Personal Devices Guidance for Visitors
- Social Media Protocol
- Twitter Protocol