

1. INTRODUCTION

1.1 Related Policies & Procedures

- 1.1.1 Safeguarding Policy
- 2.1.1 Email Protocol (see **Appendix 1**)
- 3.1.1 Anti-Bullying Policy
- 4.1.1 Data Protection Policy
- 5.1.1 Staff Code of Conduct
- 6.1.1 Employment Handbook

1.2 Rationale

- 1.2.1 The Internet offers invaluable educational resources, but its use also presents risks, especially for young users. It is essential to minimise these risks while fostering resilience among pupils. Understanding the dangers posed by online interactions, including, for example, grooming, radicalization, bullying, and abuse, is crucial.

1.3 **Objectives** - The purpose of this policy is to enable Tudor Hall to fulfil its commitment to:

- 1.3.1 Define roles and responsibilities for online safety;
- 1.3.2 Provide clear guidance on technology use within and outside the classroom for all community members;
- 1.3.3 Implement appropriate filtering of online resources;
- 1.3.4 Foster resilience in pupils and staff when using online technology;
- 1.3.5 Educate staff on their safeguarding role regarding e-safety;
- 1.3.6 Educate parents and guardians on e-safety; and
- 1.3.7 Manage personal data effectively.

1.4 **Success Criteria**

- 1.4.1 Successful implementation of this policy will ensure that all members of the community use ICT safely and responsibly.

2. METHODOLOGY

2.1 **Implementation** - Roles and Responsibilities for Online Safety

- 2.1.1 The Deputy Head (Pastoral) serves as the school's e-safety coordinator, responsible for coordinating e-safety efforts. Regular meetings with the IT Strategy Steering Group and the Head of PSHEE will evaluate the school's

strategy and effectiveness. An annual plan, following an Online Safety audit, will be developed to integrate e-safety into safeguarding duties.

2.2 Guidance on Technology Use

2.2.1 All staff, pupils, and parents must sign the relevant Acceptable Use Agreement (AUA) annually. Students' AUAs will be administered by Tutors at the beginning of the year, while staff will sign their AUAs at the start of the academic year. Parents will also sign an AUA, acknowledging their daughter's adherence to the agreement, providing information about IT equipment, and consenting to media streaming (as applicable). These agreements can be found in the appendices as follows:

- **Appendix 2:** Student Acceptable Use Agreement (AUA)
- **Appendix 3:** Staff Acceptable Use Agreement (AUA)
- **Appendix 4:** Parent Acceptable Use Agreement (AUA)

2.3 Filtering and Monitoring

2.3.1 The school employs Smoothwall for internet filtering and monitoring, along with SENSO for Microsoft Teams chat monitoring. The network manager and the DSL (e-safety coordinator) are alerted to any safeguarding issues. The DSL will follow up any concerns in line with the Safeguarding policy.

2.4 Education and Training on Online Safety

2.4.1 Regular training on safe ICT use will be provided to pupils and staff, outlined in the annual plan and updated as needed. Staff are required to complete online safety training, and the e-safety coordinator will ensure an ongoing e-safety awareness program for pupils. Access to updates and training resources will be provided via the National Online Safety portal for both staff and parents.

2.5 Reporting Mechanisms

2.5.1 Pupils are encouraged to report concerns and have access to staff members for support. Notices reminding the pupils of who they can contact if they have a concern are displayed in all tutor based rooms and boarding houses.

2.5.2 Staff must report any concerns to the e-safety coordinator promptly using CPOMs or via email. The coordinator will assess concerns and take appropriate actions, including informing parents if necessary.

2.6 Personal Data

2.6.1 Personal data management is governed by the '*Privacy Policy*'.

2.7 Email Protocol

2.7.1 The school's email protocol is essential for maintaining efficient communication and ensuring the security of sensitive information. All staff, pupils, and parents are expected to adhere to the email protocol found in **Appendix 1**.

2.8 School Use of AI Policy

- 2.8.1 **Appendix 5** '*Use of Artificial Intelligence Policy*)' outlines the principles, guidelines, and procedures regarding the integration and utilisation of AI technologies within Tudor Hall School. This policy aims to ensure ethical and responsible use of AI, safeguarding the privacy and well-being of all stakeholders while harnessing the benefits of AI innovation to enhance teaching, learning, and administrative processes.

3. MONITORING

- 3.1 The e-safety coordinator will maintain a log of cyberbullying concerns and monitor patterns, reporting to Governors regularly. They are also responsible for ensuring all relevant network users sign AUAs.

4. EVALUATION

- 4.1 The e-safety coordinator will review the policy annually to assess its effectiveness.

5. REVIEW

- 5.1 This policy will undergo annual review to ensure relevance and effectiveness in addressing evolving online safety challenges.

Written by Director of Digital Services: August 2024
Reviewed by Head of Tudor Hall: September 2024