

1. INTRODUCTION

1.1 Related Policies & Procedures

- 1.1.1 Safeguarding Policy
- 1.1.2 Email Protocol (see **Appendix 1**)
- 1.1.3 Anti-Bullying Policy
- 1.1.4 Data Protection Policy
- 1.1.5 Staff Code of Conduct
- 1.1.6 Employment Handbook

1.2 Policy Ownership

This policy is owned by the **Deputy Head (Pastoral)**, in their capacity as the Designated Safeguarding Lead (DSL). They hold overall responsibility for online safety and safeguarding related to digital technologies. The **Director of Digital Learning and Innovation** contributes to the policy by providing technical expertise, oversight of filtering/monitoring systems, and support for staff and pupil digital education.

1.3 Rationale

- 1.3.1 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, radicalisation, bullying, and abuse, is crucial.

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

- 1.4.1 Define roles and responsibilities for online safety;
- 1.4.2 Provide clear guidance on technology use within and outside the classroom for all community members;
- 1.4.3 Implement appropriate filtering of online resources;
- 1.4.4 Foster resilience in pupils and staff when using online technology;
- 1.4.5 Educate staff on their safeguarding role regarding Online safety;
- 1.4.6 Educate parents and guardians on Online safety; and
- 1.4.7 Manage personal data effectively.

1.5 Success Criteria

- 1.5.1 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

2.1.2 The Deputy Head (Pastoral) serves as the school's online safety coordinator, responsible for coordinating online 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**

2.2.2 All staff, pupils, and parents must sign the relevant Acceptable Use Agreement (AUA) annually. Pupils' 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:** Pupil Acceptable Use Agreement (AUA)
- **Appendix 3:** Staff Acceptable Use Agreement (AUA)
- **Appendix 4:** Parent Acceptable Use Agreement (AUA)

2.3 **Filtering and Monitoring**

The school employs Smoothwall for internet filtering and monitoring, along with SENSO for Microsoft Teams chat monitoring. The network manager and the DSL (online safety coordinator) are alerted to any safeguarding issues. The DSL will follow up any concerns in line with the Safeguarding policy. Filtering and monitoring systems will be reviewed termly by the Network Manager and DSL to ensure effectiveness.

2.4 **Education and Training on Online Safety**

2.4.2 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 online safety coordinator will ensure an ongoing online 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**

2.5.2 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.

2.5.3 Staff must report any concerns to the online 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**

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

2.7 **Email Protocol**

2.7.2 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**

2.8.2 **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.

Reviewed by Director of Digital Learning and Innovation: September 2025

Approved by Education & Welfare Committee: February 2025

Reviewed by Headmistress: September 2024

Written by Director of Digital Strategy: August 2024

APPENDIX 1 - SCHOOL EMAIL USE PROTOCOL

1. INTRODUCTION

- 1.1 This protocol should be read in line with the Safe Use of Technology policy and Staff Acceptable Use Agreement. To streamline communication and ensure effective use of email, please refer to this email protocol for guidance with specific guidelines for various types of email interactions within our school community.
- 1.2 Staff should remember that all school emails are professional communication and are the property of the school. Staff should be mindful that emails may be subject to scrutiny for compliance, safeguarding, or legal purposes. Include only factually accurate information.
- 1.3 This protocol is designed to achieve several objectives: minimise email volume, enhance message clarity, and uphold professional conduct in digital communications. The following sections, each customised for communication between staff, pupils, and parents, will ensure that we are consistent in our delivery of communication to our differing audiences.
- 1.4 Please be aware that email signatures are created and administered by the IT Support department at the school. These signatures are customised according to the individual's job role and are automatically appended to all accounts.

2. COMMUNICATION BETWEEN STAFF

- 2.1 **Email frequency** - Consider alternative communication methods (e.g. meetings, shared documents) when possible, to reduce the number of emails sent to staff. For urgent matters or immediate support, please use alternative methods if appropriate, such as a phone call or an in-person conversation.
- 2.2 **Concise communication** - Use clear and concise subject lines and content to facilitate efficient communication. For example, if an email does not require a reply and is for information only, please use the prefix **INFORMATION**: within the subject line.
- 2.3 **High or Low importance** - If an email is High or Low importance, please use the appropriate prefix using the High or Low button found in the tool bar when you create a new email. High importance emails should be dealt with as a priority over other emails.
- 2.4 **Attachments** - Avoid sending large attachments via email; instead use a link from the school Shared Drive (SharePoint).
- 2.5 **Internal Out-of-Office messages** - All staff should set out-of-office messages when they are unavailable (not including teaching PPA time). Dates of absence should be included if known and an alternative contact provided for urgent matters (see Appendix I - for Out of Office templates that should be used as directed – these can also be found on the school FireFly portal).
- 2.6 **Use of distribution lists** - Emails should be sent to relevant distribution lists when the information is for a group audience; however, consider whether it may be more appropriate to send information to notices@tudorhallschool.com if all staff need to be aware of the information.
- 2.7 **iSAMS communications** - Staff should use the iSAMS messaging tool to contact teachers of specific pupils. iSAMS should **not** be used to contact multiple parents; this must be done through the Head of Operations and MySchoolPortal software.

- 2.8 **Email communications with new staff before appointment** - When emailing multiple new members of staff using their personal email addresses, BCC should be employed within the email to protect email addresses.

3. COMMUNICATION WITH PUPILS

- 3.1 **Email frequency** - Staff should consider whether a different form of communication may be more appropriate.
- 3.2 **Emails for academic purposes** - Emails should be used primarily for academic matters, such as classwork updates, class announcements, and academic support. Appropriate language should be used and emails to pupils should always maintain a professional tone and distance.
- 3.3 **Student identification** - Emails should be clearly address to the specific pupil(s). Pupils have a number in their email address (e.g. jDoe30@tudorhallschool.com) which is linked to the year in which the pupil would leave the school if they stayed through to the end of sixth form.
- 3.4 **Use of school Email** - All email communication with pupils should be conducted through school-issued email accounts only.
- 3.5 **Attachments** - Pupils should be encouraged to use sharing software such as Microsoft SharePoint or Teams, reducing the need for email attachments.
- 3.6 **Response time** - Teachers should aim to respond to pupil emails within 36 hours during term time. Teachers should reply to pupils during normal working hours unless an explicit arrangement has been made for contact outside these times.

4. COMMUNICATION WITH PARENTS

- 4.1 **Centralised communication** - Information should be consolidated into newsletters or announcements where possible to reduce the frequency of parent emails. For example, for emails to a number of parents, information should be sent to the Director of Operations, who will send out the information through MySchoolPortal.
- 4.2 **External Out-of-Office messages** - All staff should set out-of-office messages when they are unavailable (not including teaching PPA time). Dates of absence should be included if known and an alternative contact provided for urgent matters (see Appendix I - for Out of Office templates that should be used as directed). At the end of each half term/term a holiday Out of Office message should be used (See appendix I - for Holiday Out of Office templates for all staff).
- 4.3 **Response time** - Teachers should respond to parents within 48 hours during a regular working week in term time. If required, a holding email should be sent to allow time to find out more information. It is the expectation that, where possible, staff check email at least once a day during term/work hours.
- 4.4 **Privacy and confidentiality** - Caution should be exercised with sensitive or confidential information. Information that the recipient does not need to know should be removed when forwarding an email. Secure channels should be used; however, staff should engage in face-to-face communication when required. When emailing multiple parents, appropriate school systems should be used.
- 4.5 **Attachments** - Parents should be encouraged to use designated platforms or portals for accessing important documents and resources. If attaching a document, or link to a document, staff should ensure that these are appropriate for the audience and do not contain personal data pertaining to others.

- 4.6 **Professional tone** - A professional and respectful tone should be maintained in all email interactions with parents. Staff should avoid using slang or overly casual language.
- 4.7 **Subject line clarity** - Staff should ensure that the subject line is clear, concise, and relevant to the content of the email so that recipients quickly understand the purpose of the message.
- 4.8 **Formal greetings** - Staff should begin emails with a professional greeting that is appropriate for the recipient's status or relationship with you. Staff should check the correct form of address for the recipient on iSAMs.
- 4.9 **Clear and concise language** - Staff should ensure that emails are direct and to the point.
- 4.10 **Grammar and spelling** - Staff should ensure that email content is free from grammatical errors and spelling mistakes. To maintain a polished and professional appearance.
- 4.11 **Appropriate formatting** - Appropriate formatting should be used, such as paragraphs and bullet points, to make email easy to read.
- 4.12 **Acknowledgment of received information** - If the email requires a response or action, staff should explicitly mention this in the closing remarks. For example, use phrases such as 'I look forward to hearing from you' or 'Please let me know your thoughts on this matter' could be used.
- 4.13 **Polite closing** - Staff should end emails politely using a sign off such as 'Best wishes', 'Sincerely', or 'Kind regards'. Staff should choose a sign off that aligns with the formality of the email.
- 4.14 **Review before sending** - Before sending, staff should review the email to ensure it aligns with the protocol outlined above.
- 4.15 **CPOMs** - Staff should record significant correspondence with parents/guardians about pastoral or academic matters on CPOMs within 24 hours, linking the post to the appropriate staff members and contacting the DSL or a DDSL for guidance if required.
- 4.16 **Email Tone** - Email should not be used when you are trying to convey complex feelings or to explore emotive issues. Emails are easy to misinterpret and may cause offence where none was intended. Consider saving an email written when tired, frustrated or annoyed and reviewing it the next day. Do not use email to reprimand or chastise, nor to convey bad news of a serious nature to an individual unless there is absolutely no alternative. By adhering to this email protocol, we aim to foster more efficient, professional, and respectful email communication within our school community. We appreciate your cooperation in helping us achieve these goals.

5. OUT OF OFFICE TEMPLATES

- 5.1 (Please update the required information in the square brackets [])

5.2 Generic message for being out of school (internal and external for dates other than end of term)

5.2.1 Thank you for your email. I am currently not in school. If you require immediate assistance in my absence, please contact [line manager/other relevant member of department] on [email address or contact number] who will be able to deal with your enquiry. Otherwise, I will respond as soon as possible after my return on [return to work date].

With best wishes

[name]

5.3 Part time members of staff (Should have an 'out of office' message on continuously)

5.3.1 Thank you for your email. As a part time member of staff my working pattern is: [Working pattern]. If you require assistance in my absence, please contact [Line manager/other relevant member of department] on [email address or phone number], otherwise, I will respond as soon as possible.

With best wishes

[name]

5.4 Boarding staff

5.4.1 Thank you for your email. Please note that my time off is [Add time off] and I am currently not on duty. If you require immediate assistance in my absence, please contact [house email address] otherwise, I will respond as soon as possible on my return.

With best wishes

[name]

5.5 Holiday Out of Office templates for all staff

5.5.1 Summer holidays

Our girls and staff are currently on summer holidays, enjoying some well-deserved rest. Reception is not operational during the summer, but if your matter requires immediate attention, please telephone +441295263434 during office hours **9.00am – 5.00pm**, and one of the team in school will assist you. Please note that the school is not open on Bank Holiday [Bank holiday date].

I am now away from school for the summer and will attend to your email promptly upon my return on [the date you will return to work].

Best wishes

[Name]

T

5.5.2 **October half term**

Thank you for your email. After a full and exciting start to the academic year, the girls and staff are now enjoying a break for half term. Reception is not operational during the half term, but if your matter requires immediate attention, please telephone +441295263434 during office hours **9.00am – 5.00pm**, and one of the team in school will assist you. Otherwise, I will respond as soon as possible after my return on [date of return to work].

With best wishes for a lovely half term break from all at Tudor Hall,

[Name]

5.5.3 **Christmas holidays**

Thank you for your email.

The school term ended on [End date of term] and the girls and staff are now enjoying a break with their families before returning on [Start of term date]. Reception is not operational during the Christmas break, but if your matter requires immediate attention, please telephone +441295263434 during office hours **9.00am – 5.00pm**, and one of the team in school will assist you. Please note School will be closed completely between [School closed dates].

Otherwise, I will respond as soon as possible after my return on [the date you will return to work].

With best wishes for a happy Christmas from all at Tudor Hall,

[Name]

5.5.4 **February half term**

Thank you for your email. Following a busy half term since Christmas, both our girls and staff are currently on a half term break, enjoying some well-deserved rest. Reception is not operational during the half term, but if your matter requires immediate attention, please telephone +441295263434 during office hours **9.00am – 5.00pm**, and one of the team in school will assist you. Otherwise, I will respond as soon as possible after my return on [date of return to work].

With best wishes,

[Name]

5.5.5 **Easter holidays (external)**

Thank you for your email. After a long and busy term our girls and staff are currently enjoying a well-deserved break for the Easter holidays. Reception is not operational during the Easter break, but if your matter requires immediate attention, please telephone +441295263434 during office hours **9.00am – 5.00pm**, and one of the team in school will assist you. Otherwise, I will respond as soon as possible after my return on [date of return to work].

Please note the school will be closed between [School closed dates].

With best wishes for a happy Easter from all at Tudor Hall,

[Name]

5.5.6 **May half term**

Thank you for your email. Both our girls and staff are currently on a half term break, enjoying some well-deserved rest. Reception is not operational during the half term, but if your matter requires immediate attention, please telephone +441295263434 during office hours **9.00am – 5.00pm**, and one of the team in school will assist you. Otherwise, I will respond as soon as possible after my return on [date of return to work].

With best wishes,

[Name]

APPENDIX 2 - PUPIL ACCEPTABLE USE AGREEMENT (AUA)

1. SECURITY

- 1.1 I will only log onto the school network, other systems and resources (e.g. Smoothwall and Office 365) with my own username and password. I will keep my account information secure and not share my password with anyone. I will report any suspicious activity regarding my account immediately to the IT Support department.
- 1.2 I will only use my assigned user account and password and will not attempt to access others' accounts, files, or data. Attempting to gain unauthorised access to accounts, files, or data will result in sanctions.
- 1.3 I will not attempt to get around the Internet filtering system (Smoothwall) if using my own laptop. The use of VPNs, proxy servers, or other circumvention tools is strictly prohibited.
- 1.4 I will not use my phone as a hotspot device, to access the Internet.
- 1.5 I will not attempt to get around the security of any host, network or account, or penetrate security measures ('hacking') on or accessed through the school network.
- 1.6 I must not probe, scan or test the vulnerability of the network or other networks.
- 1.7 I will only store schoolwork on OneDrive (SharePoint or OneNote, as appropriate) and not on my laptop's hard drive, other platforms like google drive, iCloud etc, or USB memory stick or portable hard drives.
- 1.8 If I accidentally delete a file, or files, in my folder or a shared area, I will inform the IT Support department immediately so that it can be recovered. (Deleted files are recoverable for up to 90 days).
- 1.9 If I receive anything electronically on any device I own that I am unsure of, including suspicious emails, links, or attachments, I will promptly report it to IT Support. This includes being vigilant against common cyber threats such as phishing attempts, malware, ransomware, and suspicious website links (They may contain viruses that may cause loss of data or damage to the school network).
- 1.10 I will report lost or stolen devices promptly to ensure the security of school resources.

2. PRIVACY

- 2.1 Before taking photos, filming or recording staff or other pupils, I will ask permission first from the person(s) concerned. Any media must only be stored for school purposes and must not be shared outside the school network without explicit permission.
- 2.2 If a photo or film I wish to make includes people whose permission I do not have (for example, there is a crowd of other pupils in the background), I understand that I am not allowed to film / photograph.
- 2.3 I understand that I am not allowed to create or share media (for example videos, images etc) which might be viewed as in any way indecent, rude or offensive.
- 2.4 I will not create or share media which is illegal e.g. abusive or intolerant.

- 2.5 I will respect the privacy and ownership of others' work.
- 2.6 I understand that all my use of the Internet, email, and other related technologies whilst in school or through school systems is monitored, logged and can be made available to Tudor Hall school staff.
- 2.7 For further information, I can refer to the school privacy notice (found on the school FireFly page).

3. COMMUNICATIONS

- 3.1 I will only use my school email address when communicating with staff. I will use appropriate language and adhere to professional and respectful communication practices when using school-provided email or any other communication tools.
- 3.2 I will consider the file size of attachments, understand the differences between emailing a link and attaching a file and use the most suitable method.
- 3.3 I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- 3.4 I will report any unpleasant material or message sent to me to my tutor and if necessary, the IT support department. This will help to protect the other pupils in the school as well as myself.

4. RESPONSIBLE USE

- 4.1 I understand that cyberbullying and harassment through any digital means, including but not limited to social media, email, instant messaging, or online forums, are strictly prohibited. I realise that if I fail to adhere to this, I will face sanctions. Any incidents of cyberbullying, including through social media or messaging platforms, must be reported immediately.
- 4.2 I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to a member of staff.
- 4.3 I will ensure that my online activity, both in school and outside school, will not cause staff, pupils or others distress or bring the school or its members into disrepute. This includes refraining from posting or sharing any offensive, harmful, or misleading content online.
- 4.4 I will only use my mobile phone in accordance with the school's guidelines. I will not use it in any way that causes harm or distress to others.
- 4.5 I will immediately comply with any teacher's request to shut down or close the screen of my device, when using equipment in class.
- 4.6 If permitted to use media streaming services (e.g. BBC iPlayer, Netflix), I will do so responsibly, accessing age-appropriate media.
- 4.7 Printers are provided for my use. I will use these sparingly and for educational purposes only.

- 4.8 To save resources, I will proofread my work before printing and will check the layout using the 'Print Preview' facility before printing. I understand that printer use is recorded and monitored, and misuse of a printer will be dealt with accordingly.

5. USE OF AI (ARTIFICIAL INTELLIGENCE) IVS, VS AND SIXTH FORM

- 5.1 The purpose of this section is to explain how you can use Artificial Intelligence (AI) technologies responsibly and safely at school.
- 5.2 I will use AI technologies in a way that includes and respects everyone, treating others fairly and with kindness.
- 5.3 I will protect my privacy and keep personal information safe when using AI tools, I will not post personal information into any AI software.
- 5.4 I will use AI technologies to help me learn and grow, not to cheat or take shortcuts in my schoolwork, prep or examinations.
- 5.5 If I utilise AI technologies in any of my work, I will ensure to appropriately reference the software used and adhere to the guidelines outlined in the JCQ (Joint Council for Qualifications) guidance, especially for exam specific work.
- 5.6 I will maintain transparency in acknowledging the role of AI in any assignments.

6. CARE OF SCHOOL EQUIPMENT

- 6.1 I will use school-provided devices and software responsibly and only for school-related purposes. I will ensure the devices are turned off and charged overnight when required and treated with respect.
- 6.2 I will not write on, or otherwise mark, school provided devices.
- 6.3 I will not install or use unauthorized software, applications, or extensions on school devices without proper authorization.
- 6.4 I will report any technical issues or damage to the IT department immediately.
- 6.5 I will not attempt to change or remove software.
- 6.6 I will not create or upload computer viruses.
- 6.7 I will not delete others' files.

If I am worried about being stalked, bullied or cyberbullied, or about any aspect of my experiences online, I can approach a member of staff.

I understand that this agreement is designed to keep me safe and that if it is not followed, school sanctions will be applied, and my parent/carer may be contacted. By breaking the agreement, my account may be inspected, and my network access stopped. I may also be liable to sanction from the house staff up to and including permanent exclusion.

For advice and support on staying safe online, pupils can visit www.childline.org.uk.

Further information and resources are also available at www.thinkuknow.co.uk.

APPENDIX 3 - STAFF ACCEPTABLE USE AGREEMENT (AUA)

1. INTRODUCTION

- 1.1 All adults working on the IT network, with ICT equipment and / or with laptops at Tudor Hall School must ensure that this Acceptable Use Agreement is read in conjunction with the Staff Code of Conduct and the Safe Use of Technology Policy.

2. SECURITY

- 2.1 I will only use my own username and password to log onto the school network and other systems and resources (e.g. Smoothwall and Office 365), unless a generic account has been provided by the school.
- 2.2 I will always use school supplied computer equipment where available.
- 2.3 I will not leave a computer unattended without either locking it (Win key + L) or logging off.
- 2.4 I will not attempt to bypass the internet filtering system (Smoothwall).

I will not attempt to circumvent security of any host, network or account, or penetrate security measures ('hacking') on or accessed through the school network (e.g. by attempting to use a VPN).
- 2.5 I must not probe, scan or test the vulnerability of the network or other networks.
- 2.6 I will only store materials related to school including lesson resources, pupil information or work on OneDrive or SharePoint, as appropriate.
- 2.7 I will not store school data on an external storage devices (e.g. memory stick or portable hard drive), or a private sharing service (Google Drive, Dropbox etc) unless for specific reasons as approved by IT Support/SLT, for example sending data to exam boards.
- 2.8 If I accidentally delete a file, or files, in my folder or a shared area, I will inform the IT support department immediately so that it can be recovered. (Deleted files are recoverable for up to 90 days).
- 2.9 I will not download or open file attachments or click links in emails, unless I am certain of both their content and origin. (File attachments may contain viruses that may cause loss of data or damage to the school network).
- 2.10 I am aware that cyber security is everyone's responsibility, and I will promptly report any concerns or suspicious online activities I encounter to IT Support.

3. PRIVACY

- 3.1 I will not release personal details including phone numbers, or personal email addresses of any colleague or pupil over the internet, without permission.
- 3.2 I am aware of the protocol for using photographs of children.

- 3.3 I understand that I am not allowed to create or share media which might be viewed as in any way abusive, indecent, intolerant or illegal.
- 3.4 I will respect the privacy and ownership of others' work.
- 3.5 I understand that my use of the Internet, email, and other related technologies is monitored and logged, and that the school has the right to access all user areas on the school network at any time.
- 3.6 For further information, I can refer to the school privacy notice.

4. COMMUNICATIONS

- 4.1 I will follow the email protocol. I will avoid discussing sensitive matters via email where possible and instead use approved secure channels.
- 4.2 I will only use my school email address for school-related work and communication with pupils.
- 4.3 Official communication with parents, guardians and carers will be sent through MySchoolPortal via the Head of Co-curricular and Communications.
- 4.4 I will only use the school's approved systems to communicate with pupils, and only do so for teaching and learning purposes.
- 4.5 I will ensure that all electronic communications including email, shared files including photographs and videos, messaging and social networking comply with my professional role and that electronic messages cannot be misunderstood or misinterpreted.
- 4.6 I will consider the file size of attachments, understand the differences between emailing a link and attaching a file and use the most suitable method.
- 4.7 I will not include offensive or abusive language in my messages or any other language which could be considered defamatory, obscene, menacing or illegal. I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority.
- 4.8 I will ensure that nothing in a message could be interpreted as slanderous or false.
- 4.9 I will be mindful that school email is subject to the Data Protection Act.
- 4.10 I will not send any message(s) which is/are likely to cause annoyance, inconvenience or needless anxiety.
- 4.11 I will not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes.

5. RESPONSIBLE USE

- 5.1 I will use the school's digital technology resources and systems for uses deemed 'reasonable' by the Headmistress and Governing Body.

- 5.2 I will report all accidental access to, or receipt of, inappropriate materials or any filtering breach to the DSL or deputy DSL or equipment failure to the IT Support department.
- 5.3 I will ensure that my online activity, both in school and outside school, will not cause distress to others, or bring the school or its members into disrepute, including through uploads of images, video, sounds or texts. I understand that network activity is logged on Smoothwall and accessing illegal material may result in the authorities being called to investigate.
- 5.4 I will only use my mobile phone in accordance with the school's guidelines. I will not use it in any way that causes harm or distress to others.
- 5.5 To save resources, I will proofread before printing and will check the layout using the 'Print Preview' facility before printing. I understand that printer use is recorded and monitored, and misuse of a printer will be dealt with accordingly.
- 5.6 I will not reproduce copyright materials without first getting permission from the owner. Many people will make their work freely available for education on request. Acknowledge sources on resources used.
- 5.7 I will periodically check my user areas and delete unnecessary files in both my OneDrive and on SharePoint.
- 5.8 I understand my use of the Internet and Microsoft Office applications including Teams is monitored in line with our Safe Use of Technology policy.
- 5.9 I understand my use of the Internet and features of Microsoft Office must be in line with the Staff Code of Conduct.

6. USAGE OF GENERATIVE ARTIFICIAL INTELLIGENCE (AI) TECHNOLOGIES

- 6.1 I will use AI technologies in a manner that promotes inclusivity, diversity, and avoids any form of bias or discrimination.
- 6.2 To ensure privacy of individuals, I will not enter personal and sensitive data into generative AI tools. Any data entered should not be identifiable and should be considered released to the internet.
- 6.3 If I use AI technologies in my teaching practice, I will use the technology to enhance pupil learning experiences, foster critical thinking, and encourage creativity.
- 6.4 If I require further guidance, I will refer to the Safe Use of Technology Policy which includes the school use of AI policy.

7. CARE OF SCHOOL EQUIPMENT

- 7.1 I will ensure that school-provided devices and software are predominantly used for Tudor-related tasks and responsibilities. It's important to take care of school equipment and refrain from using it for non-Tudor work-related matters. Checking personal emails and attending to other personal matters is acceptable.
- 7.2 I will not install or use unauthorized software, applications, or extensions on school devices without proper authorization.

- 7.3 I will report any technical issues or damage to the IT Support Department immediately.
- 7.4 I will not attempt to change or remove software.
- 7.5 I will not create or upload computer viruses.
- 7.6 I will not delete others' files.
- 7.7 **When using the Internet, Firefly or email with pupils**
 - 7.7.1 I will reinforce the rules for using the Internet, Firefly and email with pupils.
 - 7.7.2 I am aware of issues relating to cyber-bullying and will watch for evidence of any distress caused by the use of ICT and will investigate its cause.
 - 7.7.3 I am aware of my responsibilities with regard to ICT referred to in the Safe Use of Technology Policy.
 - 7.7.4 I have read and understood the '*Acceptable Use Agreement*' and agree to follow the eSafety rules and to support the safe use of ICT at Tudor Hall School.
 - 7.7.5 When pupils are using their own laptops in the classroom I will remind them of their Acceptable Usage Agreement and will do my best to monitor their usage as part of normal classroom behaviour management.
 - 7.7.6 Failure to adhere to this agreement may result in disciplinary action in line with school policies. This may include restricted IT access, formal warnings, or further steps as required.

PARENT/GUARDIAN ACCEPTABLE USE AGREEMENT (AUA)

1. TODD & IIS

1.1 **Laptop Usage:**

- Laptops are provided for classroom learning and preparation activities when required. Pupils need to ensure their devices are regularly updated and that they arrive to lessons with a charged device.

1.2 **Internet Access:**

- Pupils are only permitted to access the internet through the school network. The use of VPNs, proxy servers, or any other means to bypass school security measures is prohibited.

1.3 **Content Restrictions:**

- Age-appropriate filters are in place to ensure a safe browsing experience.
- Access to streaming websites, online shopping, and gaming sites are blocked during the school day. Social Media platforms are blocked at all times.
- Temporary access to these sites may be granted for specific educational purposes under staff supervision.
- Parents are encouraged to use parental controls on personal accounts to ensure age-appropriate content access at home.

1.4 **Break and Tea Time:**

- During break and tea time, pupils do not have internet access, however this may be granted for school specific purposes.

1.5 **Mobile Phones:**

- Pupils are not permitted to use their phones during the school day.

1.6 **'Phone Time' in the Evenings:**

- During designated 'phone time' in the evenings, pupils have enhanced, age appropriate, access to the internet.
- All devices must be handed in overnight for safekeeping.

1.7 **AI & Academic Integrity:**

- AI tools (such as ChatGPT) may be used in conjunction with the pupil AUA and must be used responsibly to support learning. They must not be used to complete work dishonestly. Teachers will guide pupils on appropriate AI usage if required, to develop academic integrity.

1.8 **Email and Messaging:**

- Pupils may have access to school-provided email accounts and messaging platforms for communication. Please monitor your child's communication and encourage respectful interactions.

1.9 **File Storage and Data Privacy:**

- Pupils will be provided with access to cloud-based storage solutions (For example OneDrive and OneNote) for storing and sharing educational materials. Please ensure your child uses these platforms responsibly and respects others' privacy. School – issued accounts should not be used for non-educational purposes.

- 1.10 **Cybersecurity Awareness:**
 - Please discuss cybersecurity best practices with your child, including protecting personal information, avoiding suspicious links, and reporting any security concerns to school staff.
- 1.11 **Digital Citizenship:**
 - Encourage your child to practice responsible digital citizenship by respecting intellectual property rights, practicing online etiquette, and promoting a positive online community.
- 1.12 **Parental Involvement:**
 - Try to stay involved in your child's digital life by monitoring their online activities, discussing internet safety, and supporting their digital literacy development.
- 1.13 **Reporting Procedures:**
 - If you have any concerns about your child's IT usage or encounter any IT-related issues, please alert the school.
- 2. IIIs
 - 2.1 **Laptop Usage:**
 - Laptops are provided for classroom learning and preparation activities when required. Pupils need to ensure their devices are regularly updated and that they arrive to lessons with a charged device.
 - 2.2 **Internet Access:**
 - Pupils are only permitted to access the internet through the school network. The use of VPNs, proxy servers, or any other means to bypass school security measures is prohibited.
 - 2.3 **Content Restrictions:**
 - Age-appropriate filters are in place to ensure a safe browsing experience.
 - Access to streaming websites, social media platforms, online shopping, and gaming sites are blocked during the school day.
 - Temporary access to these sites may be granted for specific educational purposes under staff supervision.
 - Parents are encouraged to use parental controls on personal accounts to ensure age-appropriate content access at home.
 - 2.4 **Break and Tea Time:**
 - During break and tea time, pupils do not have internet access, however this may be granted for school specific purposes.
 - 2.5 **Mobile Phones:**
 - Pupils are not permitted to use their phones during the school day.
 - 2.6 **'Phone Time' in the Evenings:**
 - During designated 'phone time' in the evenings, pupils have enhanced, age appropriate, access to the internet.
 - All devices must be handed in overnight for safekeeping.

- 2.7 **AI & Academic Integrity:**
- AI tools (Such as ChatGPT) may be used in conjunction with the Pupil AUA and must be used responsibly to support learning. They must not be used to complete work dishonestly. Teachers will guide pupils on appropriate AI usage if required, to develop academic integrity.
- 2.8 **Email and Messaging:**
- Pupils may have access to school-provided email accounts and messaging platforms for communication. Please monitor your child's communication and encourage respectful interactions.
- 2.9 **File Storage and Data Privacy:**
- Pupils will be provided with access to cloud-based storage solutions (for example OneDrive and OneNote) for storing and sharing educational materials. Please ensure your child uses these platforms responsibly and respects others' privacy. School – issued accounts should not be used for non-educational purposes.
- 2.10 **Cybersecurity Awareness:**
- Please discuss cybersecurity best practices with your child, including protecting personal information, avoiding suspicious links, and reporting any security concerns to school staff.
- 2.11 **Digital Citizenship:**
- Encourage your child to practice responsible digital citizenship by respecting intellectual property rights, practicing online etiquette, and promoting a positive online community.
- 2.12 **Parental Involvement:**
- Try to stay involved in your child's digital life by monitoring their online activities, discussing internet safety, and supporting their digital literacy development.
- 2.13 **Reporting Procedures:**
- If you have any concerns about your child's IT usage or encounter any IT-related issues, please alert the school.
3. **IVs**
- 3.1 **Laptop Usage:**
- Laptops are used/provided for classroom learning and preparation activities when required. Pupils need to ensure their devices are regularly updated and that they arrive to lessons with a charged device.
- 3.2 **Internet Access:**
- Pupils are only permitted to access the internet through the school network. The use of VPNs, proxy servers, or any other means to bypass school security measures is prohibited.
- 3.3 **Content Restrictions:**
- Age-appropriate filters are in place to ensure a safe browsing experience.
 - Access to streaming websites, social media platforms, online shopping, and gaming sites are blocked during the school day.
 - Temporary access to these sites may be granted for specific educational purposes under staff supervision.

Parents are encouraged to use parental controls on personal accounts to ensure age-appropriate content access at home.

3.4 Mobile Phones:

- Pupils are not permitted to use their phones during the school day.

3.5 'Phone Time' in the Evenings:

- During designated 'phone time' in the evenings, pupils have enhanced access to the internet.
- All devices must be handed in overnight for safekeeping.

3.6 AI & Academic integrity:

- AI tools (Such as ChatGPT) may be used in conjunction with the Pupil AUA and must be used responsibly to support learning. They must not be used to complete work dishonestly. Teachers will guide pupils on appropriate AI usage if required, to develop academic integrity.

3.7 Email and Messaging:

- Pupils may have access to school-provided email accounts and messaging platforms for communication. Please monitor your child's communication and encourage respectful interactions.

3.8 File Storage and Data Privacy:

- Pupils will be provided with access to cloud-based storage solutions (For example OneDrive and OneNote) for storing and sharing educational materials. Please ensure your child uses these platforms responsibly and respects others' privacy. School – issued accounts should not be used for non-educational purposes.

3.9 Cybersecurity Awareness:

- Please discuss cybersecurity best practices with your child, including protecting personal information, avoiding suspicious links, and reporting any security concerns to school staff.

3.10 Digital Citizenship:

- Encourage your child to practice responsible digital citizenship by respecting intellectual property rights, practicing online etiquette, and promoting a positive online community.

3.11 Parental Involvement:

- Try to stay involved in your child's digital life by monitoring their online activities, discussing internet safety, and supporting their digital literacy development.

3.12 Reporting Procedures:

- If you have any concerns about your child's IT usage or encounter any IT-related issues, please alert the school.

4. Vs

4.1 Laptop Usage:

- Laptops are used/provided for classroom learning and preparation activities when required. Pupils need to ensure their devices are regularly updated and that they arrive to lessons with a charged device.

4.2 **Internet Access:**

- Pupils are only permitted to access the internet through the school network. The use of VPNs, proxy servers, or any other means to bypass school security measures is prohibited.

4.3 **Content Restrictions:**

- Age-appropriate filters are in place to ensure a safe browsing experience.
- Access to streaming websites, social media platforms, online shopping, and gaming sites are blocked during the school day.
- Temporary access to these sites may be granted for specific educational purposes under staff supervision.
- Parents are encouraged to use parental controls on personal accounts to ensure age-appropriate content access at home.

4.4 **Mobile Phones:**

- Pupils are not permitted to use their phones during the school day, However, they will be able to collect from 3:45pm.

4.5 **'Phone Time' in the Evenings:**

- During designated 'phone time' in the evenings, pupils have enhanced access to the internet.
- All devices must be handed in overnight for safekeeping.

4.6 **AI & Academic integrity:**

- AI tools (Such as ChatGPT) may be used in conjunction with the Pupil AUA and must be used responsibly to support learning. They must not be used to complete work dishonestly. Teachers will guide pupils on appropriate AI usage if required, to develop academic integrity.

4.7 **Email and Messaging:**

- Pupils may have access to school-provided email accounts and messaging platforms for communication. Please monitor your child's communication and encourage respectful interactions.

4.8 **File Storage and Data Privacy:**

- Pupils will be provided with access to cloud-based storage solutions (for example OneDrive and OneNote) for storing and sharing educational materials. Please ensure your child uses these platforms responsibly and respects others' privacy. School – issued accounts should not be used for non-educational purposes.

4.9 **Cybersecurity Awareness:**

- Please discuss cybersecurity best practices with your child, including protecting personal information, avoiding suspicious links, and reporting any security concerns to school staff.

4.10 **Digital Citizenship:**

- Encourage your child to practice responsible digital citizenship by respecting intellectual property rights, practicing online etiquette, and promoting a positive online community.

4.11 Parental Involvement:

- Try to stay involved in your child's digital life by monitoring their online activities, discussing internet safety, and supporting their digital literacy development.

4.12 Reporting Procedures:

- If you have any concerns about your child's IT usage or encounter any IT-related issues, please alert the school.

5. SIXTH FORM

5.1 Internet Access:

- Pupils are only permitted to access the internet through the school network. The use of VPNs, proxy servers, or any other means to bypass school security measures is prohibited.

5.2 Content Restrictions:

- Age-appropriate filters are in place to ensure a safe browsing experience.

5.3 Computer devices and mobile phones:

- Pupils are trusted to have access to their devices and to the Internet during the school day. Internet access is turned off overnight.

5.4 AI & Academic integrity

- AI tools (Such as ChatGPT) may be used in conjunction with the Pupil AUA and must be used responsibly to support learning. They must not be used to complete work dishonestly. Teachers will guide pupils on appropriate AI usage if required, to develop academic integrity.

5.5 Email and Messaging:

- Pupils may have access to school-provided email accounts and messaging platforms for communication. Please monitor your child's communication and encourage respectful interactions.

5.6 File Storage and Data Privacy:

- Pupils will be provided with access to cloud-based storage solutions (For example OneDrive and OneNote) for storing and sharing educational materials. Please ensure your child uses these platforms responsibly and respects others' privacy. School – issued accounts should not be used for non-educational purposes.

5.7 Cybersecurity Awareness:

- Please discuss cybersecurity best practices with your child, including protecting personal information, avoiding suspicious links, and reporting any security concerns to school staff.

5.8 Digital Citizenship:

- Encourage your child to practice responsible digital citizenship by respecting intellectual property rights, practicing online etiquette, and promoting a positive online community.

5.9 Parental Involvement:

- Try to stay involved in your child's digital life by monitoring their online activities, discussing internet safety, and supporting their digital literacy development.

5.10 **Reporting Procedures:**

- If you have any concerns about your child's IT usage or encounter any IT-related issues, please alert the school.

6. TO SUPPORT INTERNATIONAL PUPILS

6.1 We will accommodate different access times to allow international pupils to contact their families. Pupils should discuss their needs with their house staff.

6.2 **Devices to be used in school**

- If your daughter has been provided with a device through the school leasing scheme, she should use this in all lessons, prep and clubs.
- If she has not been issued with a school leased device, she will be required to bring her own laptop to school to support her studies. The laptop will be used under the teacher's guidance and supervision, and appropriate web filtering will be applied whilst on school premises.
- As stated in our '*Acceptable Use Agreement*', pupils are expected to save their work using school based software such as Microsoft Office 365 applications OneDrive and OneNote, which securely stores files in the Microsoft Cloud.

6.3 Any other laptop other than the school leased device should be capable of running the following:

- Microsoft Office 365 (your daughter will receive this free as a part of our Microsoft licensing). This should be downloaded to take advantage of the full functionality.
- • An internet browser such as Google Chrome or Microsoft Edge.
- • Suitable virus protection, such as MacAfee or AVG.
- Microsoft Windows laptops are preferred. An iPad or Chromebook is not recommended
- We recommend that a laptop with an Intel i5 processor, 8GB of RAM and a good battery life will suit your daughter's requirements. We also recommend a solid-state drive (SSD) of at least 256GB as this will greatly improve the speed with which the laptop operates.

6.4 If you are unsure about whether a particular device is permitted at school, please get in touch with the Deputy Head (Pastoral) to clarify.

6.5 Please list your daughter's IT devices (e.g. rose gold iPhone 14):

School leased Microsoft Surface Device	Yes/No (delete as appropriate)

6.6 Accessing **streaming services e.g. Netflix and Amazon Prime**

- Boarding houses have their own accounts, allowing your daughter to watch age-appropriate content in a communal space.

- If your daughter is in Todd to IIs they must not have the usernames and passwords required to access your family's streaming services.
- Pupils in the IIIs or above are permitted to access your family's streaming service as long as parents/guardians ensure it is age appropriate.
- Bear in mind that this content may be accessed in private and that, as the account administrator, you can monitor what content is being accessed and when. If you have concerns about this, please report this to your daughter's House Team.

6.7 **IT at home**

- The school strongly encourages parents and guardians adopting similar digital boundaries at home, including time-based access and content filtering, to support consistency, safety and well-being.
- The school has put together some suggestions for IT access at home including access to additional information:
- Encourage setting screen time limits and downtime schedules, especially for apps like YouTube, TikTok, and streaming services.
- Suggest that devices are kept out of bedrooms overnight and handed in at a set time, as is done at school.

<https://www.internetmatters.org> – Parental guides and tools for setting controls.

<https://www.thinkuknow.co.uk/parents> – CEOP-backed site for online safety.

<https://www.nspcc.org.uk/keeping-children-safe/online-safety> – Safeguarding advice.

ARTIFICIAL INTELLIGENCE (AI) POLICY

1. INTRODUCTION

- 1.1 At Tudor Hall school we recognise the importance of integrating Artificial Intelligence (AI) technologies into our educational environment.
- 1.2 Through AI, we aim to offer personalised learning experiences, streamline administrative processes to free up time, and present innovative engagement methods for teachers. Concurrently, we acknowledge the ethical and safety considerations intrinsic to AI's application¹ and we recognise the importance of using these technologies in a manner that respects privacy, promotes fairness, and prevents discrimination. This policy seeks to set a robust framework for the ethical, transparent, and responsible use of AI at Tudor Hall School.
- 1.3 This policy has been updated to ensure full compliance with the Joint Council for Qualifications (JCQ) guidance on the use of AI in assessments (April 2025), including standards for authenticity, malpractice prevention, and appropriate referencing.

2. SCOPE

- 2.1 This policy applies to all AI and data technologies used in Tudor Hall School, and is extended to all the members of the school community, and should be read in conjunction with:
 - 2.1.1 Tudor Hall School IT *'Acceptable Use Agreement'* for staff or pupil;
 - 2.1.2 Tudor Hall School *'Staff Code of Conduct'*;
 - 2.1.3 Tudor Hall School *'Safe Use of Technology Policy'*; and
 - 2.1.4 *'Artificial Intelligence (AI) Use in Assessments: Protecting the Integrity of Qualifications'* Joint Council for Qualifications' (JCQ) Revision 1.
 - 2.1.5 Department for Education (DfE): Generative AI: Product Safety Expectations (2025).
 - 2.1.6 Keeping Children Safe in Education (KCSIE) 2025 – including Part 2: Online safety and filtering & monitoring expectations.
 - 2.1.7 DfE Filtering and Monitoring Standards (latest).
 - 2.1.8 This policy adopts the DfE Generative AI product safety expectations across: filtering; monitoring & reporting; security; privacy & data protection; intellectual property; design & testing; and governance.

3. PUPIL GUIDELINES

- 3.1 Integration of AI in Learning, Teaching & Assessment.
- 3.2 Pupils may use AI tools to support their learning where this genuinely helps understanding and skills; however, Key Stage 3 (KS3) use of generative AI is currently not permitted. Key Stage 4 (KS4) and Key Stage 5 (KS5) use is permitted when used responsibly and only with named tools on the school's AI Tools Register, for teacher-

¹ [Teacher Development trust, Understanding AI for school Leaders, September 2023](#)

set tasks (and with supervision as appropriate). Responsible use means no personal/identifiable data, no attempts to bypass filters, check accuracy and credit AI assistance, and follow Joint Council for Qualifications (JCQ) rules—never present AI-generated work as your own (including for Non-Examined Assessments (NEAs), General Qualifications (GQs) and Vocational & Technical Qualifications (VTQs)):

3.3 These are based on the following principles:

- 3.3.1 **Verification of AI-suggested concepts and personal data** - Pupils should validate concepts suggested by AI against reputable sources, ensuring accuracy and reliability in their academic work. Personal information should not be entered into any AI software.
- 3.3.2 **Recognition of AI's limitations and biases** - Acknowledging the potential limitations (inaccurate, inappropriate, out of date or unreliable information) and biases of AI is crucial. Pupils should be discerning users, critically assessing information provided by AI tools². AI software should be used in a way that respects and treats others with fairness.
- 3.3.3 **Avoidance of plagiarism** - Pupils are prohibited from presenting AI-generated content as their original work. Plagiarism undermines academic integrity and is strictly against school policies³.
- 3.3.4 **Proper referencing of AI-derived content** - When incorporating AI-generated content into their work, pupils must appropriately reference the source, recognising that credit is given not solely based on intrinsic merit but on the contribution of the AI tool.
- 3.3.5 **Comprehensive acknowledgment of AI tools utilised** - pupils are required to provide detailed acknowledgment of the AI tools they employ. This includes maintaining records of their usage to ensure transparency and accountability in their academic endeavours.
- 3.3.6 Pupils must sign a declaration of authenticity for all NEAs and coursework, confirming that the work is their own. They must understand the consequences of false declarations, including disqualification.
- 3.3.7 Pupils must be aware that using AI to complete or edit assessments, or failing to declare its use, constitutes malpractice and will be treated as such under JCQ regulations.

4. TEACHING STAFF GUIDELINES

- 4.1 Staff play a vital role in managing the ethical and appropriate use of AI by pupils. Their responsibilities include:
 - 4.1.1 Engaging in training and staying updated on AI developments.
 - 4.1.2 Supporting pupils in the safe, creative, and responsible use of AI in classwork.
 - 4.1.3 Ensuring that no personal data is entered into generative AI tools.

² [Russell Group, *Principles On The Use Of Generative AI Tools In Education*, July 2023](#)

³ [Office of Educational Technology, *Artificial Intelligence and the Future of Teaching and Learning*, May 2023](#)

- 4.1.4 Monitoring pupil work for signs of AI misuse.
- 4.1.5 Ensuring AI use in assessments complies with JCQ rules.
- 4.1.6 Staff must only accept work that is demonstrably the student's own. Where they have doubts, they must investigate and follow the school's internal process before authentication.
- 4.1.7 Teachers must not use AI tools as the sole means to mark student work. AI-generated analysis may supplement, but not replace, human judgement.
- 4.1.8 All teaching staff must be aware of the centre's malpractice procedures, including how AI misuse is treated, and report concerns immediately to the Head of Centre or Director of Digital Strategy.
- 4.1.9 Teachers must collaborate to refine and review the school's AI policy annually, considering emerging risks and student behaviour.

5. PUBLIC EXAMINATIONS & NON-EXAMINED ASSESSMENT (NEA):

- 5.1 During assessments, AI tools may be employed under specific conditions to genuinely reflect a pupil's independent efforts. Any instances of AI misuse, such as plagiarism or the creation of misleading references, will be treated with utmost seriousness.
- 5.2 Pupils using computers in assessments where AI use is not permitted must have internet access and AI tools disabled in line with JCQ examination requirements.
- 5.3 Where AI misuse is suspected before a declaration of authenticity is signed, it will be addressed internally and must not be submitted until resolved.

6. ENSURING ETHICAL USE OF ARTIFICIAL INTELLIGENCE AT TUDOR HALL SCHOOL

- 6.1 In our commitment to upholding ethical standards, all users of Artificial Intelligence (AI) within Tudor Hall School are expected to:
- 6.2
 - 6.2.1 **Respect privacy and intellectual property** - Demonstrate utmost respect for privacy and intellectual property rights in all AI interactions.
 - 6.2.2 **Prevent discrimination and unjust outcomes** - Refrain from actions that may lead to discrimination or unjust outcomes, fostering an environment of fairness and equity.
 - 6.2.3 **Compliance with laws and policies** - Adhere strictly to all relevant laws, regulations, and school policies, with a particular emphasis on data privacy.
 - 6.2.4 **Mitigate AI biases** - Stay informed about potential biases in AI systems and actively work towards mitigating them to ensure fairness and impartiality.
 - 6.2.5 **Stringent data governance** - Adhere rigorously to data governance norms, encompassing compliance with GDPR regulations and the school's Data Policies.

7. IMPLEMENTATION, MONITORING, AND REVIEW

- 7.1 **Vendor collaboration** - Tudor Hall School will exclusively engage with vendors that adhere to the highest ethical and technical standards in the development and deployment of AI solutions.
- 7.2 **Monitoring and feedback** - Continuous monitoring guarantees that AI systems align with our ethical commitments. Open feedback channels provide the school community with opportunities to share experiences and express concerns regarding AI usage. This should be directed to the Director of Digital Strategy and Learning and/or the IT Support department in the first instance.
- 7.3 **Education** - Regular training sessions focusing on the ethical, transparent, and safe use of AI will be organised for both staff and pupils, fostering a culture of responsible AI engagement.
- 7.4 **Review mechanism**- This policy will be reviewed at least annually or as often as necessary to address changes in laws or practices related to AI and data use. Updates will be communicated to all users in a timely manner.
- 7.5 AI Tools Register (named tools, policy stays vendor-agnostic).
- 7.6 The school keeps a live AI Tools Register listing the specific products pupils may use at KS4/KS5. To add a tool, staff submit a short request; approval requires:
- supplier confirmation they meet Department for Education (DfE) Generative AI: Product Safety Expectations;
 - a Data Protection Impact Assessment (DPIA);
 - DSL and Data Protection Officer (DPO) sign-off;
 - configuration so school filtering and monitoring work on all school accounts/devices (incl. Bring Your Own Device (BYOD) where possible).

Note: AI features built into school-managed platforms (e.g. our Microsoft 365 tenant with Single Sign-On (SSO) and Multi-Factor Authentication (MFA)) count as named when that platform appears on the Register.

- 7.7 Filtering on all devices. When pupils or staff use school accounts to access AI tools, filtering and moderation must still work on every device, including Bring Your Own Device (BYOD) such as personal phones and tablets.
- 7.8 Monitoring and reporting: Prompts and responses must be log-able; attempted access to harmful content must trigger real-time, age-appropriate notices to users and alerts to local supervisors (e.g., DSL/IT). Logs must support trend reporting without over-burdening staff.
- 7.9 Security requirements for AI tools: AI suppliers (e.g. ChatGPT) must evidence jailbreak resistance, role-based permissions, regular patching, Single Sign-On (SSO) and Multi-Factor Authentication (MFA), and safe testing before model/version upgrades.
- 7.10 Privacy and data protection: A Data Protection Impact Assessment (DPIA) is mandatory for any pupil-facing AI; publish child-friendly privacy notices; personal data must not be used to train or fine-tune models; identify and record the lawful basis for processing. Staff and pupils must not paste personal/identifiable data into generative AI unless explicitly approved in the DPIA/Record of Processing.

- 7.11 Intellectual property: No storage, collection or use of pupil or staff content for commercial purposes (including training/fine-tuning) without consent (parental where under 18).
- 7.12 Design and testing: Pilot tools with representative cohorts; capture edge cases including SEND/EAL; complete an equality impact consideration; and test model/version upgrades in a safe environment before release.
- 7.13 Governance, audit and complaints: Maintain a product-level risk assessment and AI risk register; provide a clear complaints/escalation route for AI safety issues; and keep an auditable trail of approvals, changes and incidents.

8. CONCLUSION

- 8.1 By adhering to this AI policy, all members of the Tudor Hall School community contribute to the responsible integration of AI technologies into our educational environment, fostering a culture of innovation while prioritizing the well-being and privacy of our pupils and staff.
- 8.2 This policy ensures that AI is used ethically, transparently, and to the benefit of all learners while protecting the integrity of assessments and qualifications.