ETON ACADEMY

E-Safety Policy

Version 3

Version Control	
Implementation Date	4th September 2023
Reviewed	9th September 2024
Reviewed	30th April 2025
Reviewed	4th July 2025
Next Review	September 2025

1. Introduction

1.1. Eton Academy aims to ensure that all students are safe online. IT and online communications now allow for enhanced, international learning, and unparalleled opportunities in education. Online learning can pose a different set of risks as opposed to traditional schooling, therefore, our young people are equipped with the suitable and necessary precautions in order to keep them safe when learning online. We have plans in place to help students safe in the online environments, as well as providing them with advice on mitigating risks, including bullying, harassment, grooming, abuse and radicalisation among other topics.

1.2. Technology is rapidly evolving around us, meaning there are ample opportunities to vary learning methods. Currently Eton Academy uses a mixture of the following in our school:

1.2.1. Zoom
1.2.2. Classe365
1.2.3. Google Suite
1.2.4. Websites
1.2.5. Emails and instant messaging
1.2.6. Social networking
1.2.7. Music/video downloads
1.2.8. Podcasting

1.2.9. Mobile internet devices such as smartphones and tablets, along with any applications that can be downloaded onto such devices.

1.3. This policy is implemented school-wide, and acts purely in the interest of protecting the safety of the school community. It aims to provide guidance and minimise risk wherever possible.

1.4. While the idea of online education is an exciting concept, we at Eton Academy see the need for policing and will update this document as and when appropriate. We understand the responsibility to educate students on the appropriate conduct and behaviours when learning online - we also understand the need to bridge the sometimes cultural divide, with expectations occasionally varying. Students deserve a place to voice their concerns and anxieties that come with online schooling and Eton Academy aims to assist and quell these anxieties wherever they can do so.

1.5. The following policy applies to all members of the school community, including staff, students, parents, and visitors who have access to and are users of Eton Academy's IT systems and equipment.

1.6. Both this Policy and Acceptable Use Agreements cover:

1.6.1. IT equipment and mobile devices provided by the school to members of teaching and non-teaching staff, e.g., laptops, monitors and phone systems.

1.6.2. Personal IT equipment/devices owned and used by students and visitors to the school to access our platform.

1.7. Please note that, as outlined below, staff should not be using personal equipment/devices to access school platforms.

2. Roles & Responsibilities

2.1. The Senior Leadership Team holds ultimate responsibility for ensuring compliance with the latest Keeping Children Safe in Education and Online Safety Act guidance This includes annual reviews of online safety provisions, termly reporting on filtering, monitoring, and safeguarding incidents, and ensuring the DSL is appropriately trained to oversee all online safety matters.

2.2. Designated Safeguarding Lead (DSL)

Eton Academy's DSL, Dr Gabrielle Hargreaves, is responsible to the CEO for the day-to-day issue relating to e-safety. The DSL has responsibility for ensuring this policy is upheld by all members of

the school community, and works with the relevant individuals to achieve this. They keep up to date with current e-safety issues and guidance issued by the relevant organisations.

2.3. Staff

All staff are required to sign the Acceptable Use Agreement before accessing school systems. As with all issues regarding school safety, staff members are encouraged to create a culture of listening and acceptance, and keep track of and report any safety-related incidents that may arise on a daily basis.

2.4. Students

Students are responsible for using school IT systems following the Acceptable Use Agreement, and for letting staff know if they see IT systems being misused.

2.5. Parents and Carers

The school believes that parents are pivotal in promoting e-safety and maintaining a conscious online presence. Eton Academy will always contact parents if it has any concerns about students behaviour in this area, and likewise believes that parents will feel able to share any concerns they themselves may have.

3. Education and Training

3.1. Staff: awareness and training

3.1.1. All staff receive annual training that covers the latest KCSIE updates, emerging online risks, and updates to the school's filtering and monitoring systems. Pupils receive regular age-appropriate sessions on online safety, including sextortion, online scams, and the use of generative AI.

3.1.2. All new teaching staff receive information and Acceptable Use Agreements as part of their induction.

3.1.3. All staff receive regular information regarding training on e-safety and their responsibilities as thus.

3.1.4. All staff working with children/young adults/young adults are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following all e-safety procedures. These behaviours and expectations are summarised in the Acceptable Use Agreement, which must be signed before gaining access to school IT systems.

3.1.5. Teaching staff are encouraged to incorporate e-safety activities within their subject areas, and establish a culture of talking should they arise. They should know what to do in the event of a misuse of technology by any member of the school community.

3.1.6. With the rapid adoption of Artificial Intelligence (AI) tools, Eton Academy educates pupils on the safe, ethical, and responsible use of AI, including data privacy, bias awareness, and avoiding academic dishonesty. Staff receive guidance on appropriate AI use in teaching and assessment.

3.2. Students: e-Safety in the curriculum

3.2.1. We believe it is essential for meaningful e-safety guidance to be given to students, and this is something that will be supplied in students' Induction Handbook, where students can find a variety of resources and necessary information regarding their online presence and safety.

3.2.2. Information will be provided at an age-appropriate level, and staff will ensure students feel comfortable to ask questions about their safety and that of their fellow learners, should they wish to. Information will pertain to all manner of e-safety, from password security and identity theft, to sexual exploitation and grooming.

3.2.3. Students will also be taught in their various subject classes about intellectual property and respecting other people's information.

3.2.4. Students should be aware of the impact of cyber bullying and feel free and able to seek help should they feel they are being targeted.

3.2.5. Students will also be made aware of the risks associated with misinformation, disinformation, and conspiracy theories online, and will be taught how to critically evaluate information sources to ensure accuracy and reliability.

3.3. Parents

3.3.1. Eton Academy seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about students' behaviour in this area, and likewise believes that parents will notify the school should they become concerned about anything pertaining to e-safety.

3.3.2. Eton Academy recognises that not all parents and guardians may feel equipped to protect their children/young adults when they use electronic equipment at home and would encourage parents to seek advice and support with the school at any time.

4. Use of school and personal devices

4.1. Staff

4.1.1. Staff may use personal devices to access school systems only under the conditions outlined in the Eton Academy Bring Your Own Device (BYOD) Policy. This includes approval by the IT Department, installation of required security software, and strict adherence to UK GDPR and safeguarding protocols. Staff must not store or screenshot EHCPs or other special category data locally. All such data must be accessed through encrypted cloud platforms only.

4.2. Students, Parents and Carers

4.2.1. Students will access our school platform via personal devices, which may include PCs, laptops, and mobile devices. Students and their families are responsible for the safe and appropriate use of these devices, including their security.

4.2.2. It is recommended by Eton Academy that a form of antivirus software is installed, and that parents set up privacy settings and/or content blocks so that their children/young adults cannot access inappropriate content.

4.2.3. Parents and students are required to read and sign our Acceptable Use Agreement. It is highly recommended that parents monitor the children/young adults's use of devices, particularly during the school day, and that non-school related activities are restricted to either break times or after school.

4.2.4. Eton Academy recognises that mobile - and sometimes other - devices are needed for medical purposes or as an assistant to students who may have disabilities or special educational needs (SEN). Where a student needs to use a device for such purposes, the student's parents/carers may wish to inform the school, and relevant staff members will be informed.

5. Communication - Email, Messaging, Social Media

5.1. Staff

5.1.1. Staff must not access social networking sites, personal email accounts, or any website which is unconnected to school work, or school business while teaching, or in front of students. Such access may only be made from staff members' personal devices.

5.1.2. When accessed from staff members' personal devices, staff must use social networking sites with caution, being aware of what is published online and its potential impact on their professional position and the reputation of the school.

5.1.3. The school has taken all reasonable steps to ensure that the school's main platforms, Classe365, Google Suite and Zoom are safe and secure. Staff should be aware that all communications through the schools main platforms, alongside school email addresses are monitored.

5.1.4. Staff should report immediately to the DSL the receipt of any communication that makes them feel uncomfortable, or is offensive, discriminatory, threatening, or of a bullying nature. They should not respond to any such communication. Staff must be vigilant to any fraudulent emails and should report any such emails to the senior management team.

5.1.5. Any online communications, both in and out of school, on school or personal devices, must not knowingly or recklessly:

5.1.5.1. Place a child or young person at risk of harm, or cause actual harm;

5.1.5.2. Bring the school into disrepute;

5.1.5.3. Breach confidentiality;

5.1.5.4. Breach copyright;

5.1.5.5. Breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by: - making offensive or derogatory comments relating to sex, gender, gender reassignment, race (nationality), disability, sexual orientation, religion or belief, or age. This is alongside using social media to bully another individual, or posting links to, or endorsing, material that is discriminatory or offensive.

6. Students

6.1. Students will communicate with staff members via Eton Academy email addresses. Students should be wary of content that they send to staff members - both through email and through the school's platforms, as inappropriate content could affect their place at Eton Academy.

6.2. Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature, and should report any such communication to either their teacher, another staff member or the DSL.

6.3. Whether using the school platforms, or personal social media accounts, Eton Academy wishes for students to carefully consider any information or content shared in their posts, repost or endorsement of content created by others. Content posted should not be deemed inappropriate, offensive, or likely to cause embarrassment to an individual or group. This includes content of a sexual nature, and content that is offensive or discriminatory.

6.4. Students should be aware that the storage/sharing/sending of abusive or inappropriate messages or content via their personal devices, even outside of the school platform is considered a breach of the school's Behaviour Policy. Any concerns about this will be passed on to the DSL, who will investigate further.

7. Camera Expectations

7.1. Our expectation is that teachers will use their webcam when delivering lessons online, and we also expect students to use and utilise their webcams when in lessons.

7.2. We have found that there are many benefits to students actively using their webcams, rather than taking a more passive, removed role behind a blank screen. We believe these benefits are:

7.2.1. Students feel a greater sense of community, especially given the more international aspect of Eton Academy's education

7.2.2. Teachers can interpret visual cues, and offering help to students who are perhaps struggling becomes far easier.

7.2.3. The flow of lessons is not impeded, and students can ask questions and address issues with ease.

7.3. To ensure the safety of our students, all staff members and students are required to adhere to the following guidelines:

7.3.1. Users must be dressed appropriately for all online lessons. Inappropriate clothing includes pyjamas, vest tops, see-through clothing, or items with offensive language,

imagery, or logos. Clothing should fully cover the upper and lower body and be suitable for a school setting.

7.3.2. Students should consider what is visible on their webcam. Wall displays, posters, or personal items that could be distracting or inappropriate must not be visible. A virtual background may be used for privacy if needed

7.3.3. Students should participate in lessons from a calm, quiet, and distraction-free environment. Ideally, they should be seated upright at a desk or table. Background noise such as TV or music should be avoided.

7.3.4. Cameras should remain switched on throughout the lesson unless otherwise instructed by the teacher. Students must ensure their full face is clearly visible. Other individuals, such as parents or siblings, should not appear on camera during lessons.

7.3.5. Family members should be made aware when a Zoom session is taking place. They should dress appropriately and behave respectfully if they appear in the background.

7.3.6. Recording, photographing, or taking screenshots of Zoom lessons is strictly prohibited. Meeting links must not be shared with others.

7.3.7. Use appropriate language and treat both staff and students with respect.

7.4. Eton Academy will ensure that recorded classes are securely uploaded to the school's platforms. They will be made available upon request.

7.5. All recorded lessons will be held in a secure place, should they need to be reviewed for safeguarding or academic purposes

7.6. We will store lesson recordings for the previous half term, one the new half term begins they will be deleted.

7.7. There may be times or a specific reason as to why students feel they cannot appear on webcam during lessons. If this is the case, parents are encouraged to contact the students' teacher in order to discuss the situation and their concerns. In this case, students not appearing on webcam can still make meaningful contributions to the class, using the chat function on the school's learning platform.

7.8. Eton Academy accepts that not all students and families may have access to a webcam, and if this is the case, the student or their parents should notify the school as possible.

8. Course of Action if inappropriate content is found

8.1. If inappropriate content is found (i.e., content that is pornographic, violent, racist, sexist, homophobic or horrific) the user should:

8.1.1. Turn off the monitor or minimise the window.

8.1.2. Report the incident to their teacher, responsible adult, or the DSL.

8.1.3. The teacher/responsible adult should:

8.1.4. Ensure the well-being of the student.

8.1.5. Note the details of the incident, including the web page address that was unsuitable (without showing or reshowing the content to students).

8.1.6. Report the incident to the DSL.

8.2. The DSL will then:

8.2.1. Log the incident and take any appropriate action.

8.2.2. When necessary, report the incident to parents and relevant employees at Eton university, so that additional actions can be taken.

9. Data Storage

9.1. The school takes its compliance with the Data Protection Act 2018 (UK) very seriously. Please refer to the Data Protection Policy and Acceptable Use Agreement for further details.

9.2. Staff are expected to save all documents, presentations and data relating to their work to the school platform e.g. GoogleDrive and Classe365.

9.3. Staff devices should be encrypted if any data or passwords are stored on them.

9.4. Eton academy does not endorse the use of other types of data storage, e.g. USB memory sticks, CDs portable drives; except in the case of coursework submitted as part of the IGCSE and A-Level qualifications (and this is subject to approval from Eton Academy). No personal data should be stored on any personal memory sticks, CDs or portable drives.

9.5. Any security breaches or attempts, loss of equipment and any unauthorised or suspected misuse of IT must be reported to a member of Eton Academy staff immediately.

10. Password security

10.1. Staff and students will each have an individual school login. Staff and students are regularly reminded of the need for password security.

10.2. All students and staff members should:

10.2.1. Use a strong password (usually containing 8 or more characters, upper and lower case letters, as well as numbers)

10.2.2. Not write passwords down; and

10.2.3. Not share passwords with other students or staff members.

11. Safe use of digital and video images

11.1. The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images they have recorded themselves or downloaded from the internet. However, staff, students and parents/carers need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain on the internet for forever and may cause harm and embarrassment for individuals in both the short and long term.

11.2. When using digital images, staff should inform and educate students about the risks associated with the taking, use of, and sharing and publication of digital images. In particular, they should recognise the risks attached to publishing their digital images on the internet (e.g. social networking sites).

11.3. Parents/carers and students are not permitted to record or create images of any part of the school platform, including lessons. To respect everyone's privacy, and for the protection of data, recordings and images should not be published in blogs or social networking sites.

11.4. Students may need to record or create digital images to support educational aims but must follow this policy and the Acceptable Use Policy concerning the sharing, distribution, and publication of those videos/images. Written permission will be obtained from parents or carers before photographs are published on the school, or the school's presence on social media. Photographs published on the school website or other such platforms will be carefully selected and will comply with good practice guidance on the use of such images.

11.5. Care should be taken when taking digital/video images that students are dressed appropriately and not participating in activities that may bring both the individual or institution into disrepute.

12. Misuse

12.1. Eton Academy will not tolerate illegal activities or activities that are inappropriate in the school context and will report illegal activity to the relevant local enforcement authorities. If the school discovers that a child or young person is at risk as a consequence of an online activity, it may seek external assistance. This includes, but is not limited to; involvement of cyberbullying, 'sexting' or the sharing of youth-produced sexual images, involvement in radicalisation, and other high risk activities.

12.2. The school will impose a range of sanctions on any student who misuses technology to bully, harass, or abuse another student.

13. Electronic Devices - search and deletion

13.1. Images found on a mobile phone or other electronic devices can be deleted unless it is necessary to pass them on to police or relevant local authorities. The member of staff must have regard for the local regulations and guidelines when determining what is a "good reason" for examining or erasing the contents of an electronic device. In determining a "good reason" to examine or erase files, the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, disrupt teaching or break school rules.

13.2. If inappropriate material is found on a device, the member of staff must consult with the DSL to decide whether to delete the material in question, retain it as evidence (of a criminal breach or breach of school rules), or whether the material is of such seriousness that it requires the involvement of the police.

14. Loading/installing software

14.1. For this policy, software relates to all programmes, images or screensavers, which can be downloaded or installed from any other media.

14.2. Any software loaded onto the school system or individual computers and laptop/devices must be properly licensed and free of viruses.

14.3. Where staff are authorised to download software onto their laptops/devices, they must ensure that it is consistent with their professional role and that they are satisfied that any downloaded images and video clips do not breach copyright.

15. Backup and disaster recovery

15.1. The school will define and implement a backup regime which will enable recovery of critical systems and data within a reasonable timeframe should data loss occur. This regime should include:

15.2. The use of a remote location for backup of crucial school information, either by daily physical removal in an encrypted format, or via a secure encrypted online backup system.

15.3. Staff are responsible for backing up their data on teacher laptops/devices and should utilise any system that may be enabled such as automated copying of files to the school server.

15.4. Backup methods should be regularly tested by renaming and then retrieving sample files from the backup.

15.5. Eton Academy should also define a whole school IT disaster recovery plan which would take effect when a severe disturbance to the schools IT infrastructure takes place, to enable critical school systems to be quickly reinstated and prioritised, including who would be involved in this process and how it would be accomplished.

16. Compliance, Sanctions and Disciplinary Matters

16.1. Non-compliance with this policy exposes the school to risks. If a breach of this policy occurs, the school will respond immediately by issuing a verbal then written warning to the staff member, student or parent. Guidance will also be offered.

16.2. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the user's access to our platform may be temporarily withdrawn.

16.3. For persistent breach of this policy, the school will permanently revoke permission to access school platforms.

17. Acceptable Use Policy

This policy applies to all members of the school community, including staff, students, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, senior leaders, and regular volunteers. 'Parents' includes students' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

18. Online Behaviour

18.1. As a member of the school community you should follow these principles in all of your online activities:

18.1.1. Ensure that your online communications, and any content you share online, are respectful of others.

18.1.2. Do not access, create or share content that is illegal, deceptive, or likely to offend

other members of the school community (for example, material that is obscene, or promotes violence, discrimination, or extremism).

18.1.3. Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly.

18.1.4. Do not access or share material that infringes copyright, and do not claim the work of others as your own.

18.1.5. Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.

18.1.6. Staff should not use their personal email, or social media accounts to contact students or parents, and students and parents should not attempt to discover or reach the personal email addresses or social media accounts of staff.

19. Using the school's IT systems

19.1. Whenever you use the school's IT systems you should follow these principles:

19.1.1. Only access school IT systems using your username and password. Do not share your username or password with anyone else.

19.1.2. Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not try to access parts of the system that you do not have permission to access.

19.1.3. Do not attempt to install software on, or otherwise alter, school IT systems.

19.1.4. Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.

19.1.5. Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

19.1.6. Compliance with related school policies

19.1.7. You will ensure that you comply with the school's e-Safety Policy, Mobile device and Social Media Policy, Safeguarding Policies and Counter-Bullying Policy.

20. Breaches of this policy

20.1. A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. Also, a deliberate breach may result in the school restricting your access to school IT systems.

20.2. If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online, you should report it to the school's DSL. Reports will be treated with confidence.

21. Complaints relating to all aspects of E-Safety

21.1. As with all issues of safety, if a member of staff, a student or a parent/carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Please see the Complaints Policy for further information.

22. Filtering and Monitoring Policy for Online Safety

22.1. Eton Academy recognises that effective filtering and monitoring are essential parts of our safeguarding approach and are required under the statutory guidance Keeping Children Safe in Education (KCSIE) 2025, the Online Safety Act 2023, and the Department for Education's Filtering and Monitoring Standards.

22.2. This policy applies to all students enrolled at Eton Academy, their parents/guardians, and staff involved in delivering online education.

22.3. School's Responsibility

Eton Academy takes the following steps to ensure a secure online environment during school hours:

22.3.1. Secure Platforms: We utilize secure, password-protected platforms for delivering lessons, assignments, and communications to protect students from exposure to inappropriate content.

22.3.2. In-School Filtering: Our online classroom systems are designed to block offensive language and harmful content. Moderators actively monitor chats, forums, and other interactive spaces to ensure safe communication between students and staff.

22.3.3. Monitoring and Reporting: Our teachers and staff are trained to spot any potential

issues, such as cyberbullying or exposure to harmful material, and are committed to reporting concerns to the safeguarding team immediately.

22.3.4. Online Safety Education: We provide continuous education to students about online safety, emphasising responsible internet use, recognizing dangerous content, and how to report concerns both within and outside of the virtual campus.

22.3.5. The Designated Safeguarding Lead (DSL) holds overall responsibility for ensuring filtering and monitoring systems are appropriate, effective, and meet statutory requirements.

22.3.6. The DSL works with the IT Manager and Senior Leadership Team (SLT) to review and maintain systems.

22.3.7. All staff are responsible for reporting any harmful, inappropriate, or suspicious online content immediately to the DSL or a member of the SLT.

22.4. Parents/Guardians' Responsibility

Since students attend classes from home, we expect parents/guardians to take the following steps to protect their children/young adults while learning online:

22.4.1. Home Filtering: Ensure that your home network is equipped with content filtering tools provided by your Internet Service Provider (ISP) or third-party software, which can block access to adult, offensive, or harmful content.

22.4.2. Parental Monitoring Tools: Parents are encouraged to install monitoring tools such as Net Nanny, Qustodio, or similar programs on students' devices to supervise internet activity, set time limits, and receive notifications of any inappropriate attempts to access restricted websites.

22.4.3. Device Safety: Ensure that the devices used for learning have up-to-date antivirus software and firewall protection to reduce the risk of malware or inappropriate content reaching your child's/young adult's device.

22.4.4. Supervision: While Eton Academy takes responsibility for the content delivered during classes, we encourage parents to supervise their children/young adults's broader internet usage, especially outside school hours, to ensure their safety.

22.5. Shared Responsibility

Both Eton Academy and parents/guardians share the responsibility for safeguarding students

from harmful online content:

22.5.1. Eton Academy is responsible for monitoring and securing its online learning platforms.

22.5.2. Parents/guardians are responsible for implementing and maintaining appropriate filtering and monitoring tools at home to create a safe digital environment for their children/young adults.

22.6. Annual Review and Evaluation

22.6.1. Filtering and monitoring provision is formally reviewed at least annually, with outcomes reported to the SLT and governing body.

22.6.2. The review will consider:

22.6.2.1. Effectiveness of filtering and monitoring in reducing access to harmful content.

22.6.2.2. Impact on teaching and learning.

22.6.2.3. Staff and student feedback.

22.6.2.4. Updates to statutory requirements.

22.7. Reporting Concerns

If a parent/guardian becomes aware of any inappropriate content or incidents involving their child/young adult while using Eton Academy's online learning tools, they should report it to the school immediately. Concerns can be addressed directly to our Designated Safeguarding Lead (DSL), Dr. Gabrielle Hargreaves, at gabrielle.hargreaves@eton-academy.net

Any illegal online material encountered will be reported to the relevant agencies such as the Internet Watch Foundation (IWF) or CEOP.

23. Use of Artificial Intelligence (AI) at Eton Academy

As Artificial Intelligence (AI), particularly generative AI (GenAI), becomes more prominent in education and society, Eton Academy is committed to ensuring its use is safe, ethical, responsible, and aligned with our values as an accredited online education provider.

We recognise the potential of AI to support learning, reduce teacher workload, improve school operations, and prepare students for a future where AI will play a central role. However, we are equally mindful of the risks and are implementing clear structures to support staff, students, and families in understanding and using AI responsibly.

Key Principles

23.1. We support the responsible use of AI for educational and operational purposes, encouraging staff to use school-approved AI tools to enhance planning, assessment, feedback, and administration, where appropriate.

23.2. Students will be taught how AI tools work, their benefits and limitations, and the ethical and social implications of their use. Digital literacy and AI awareness will be embedded into the curriculum where appropriate.

23.3. AI should assist but never replace human judgment. All final decisions that affect learners or staff must be made by a human.

23.4. Staff and students must not upload personal, identifiable, or sensitive information into AI tools that are not explicitly approved by the school.

23.5. Staff are expected to fact-check and critically evaluate all AI-generated outputs before sharing them.

23.6. AI tools must be compliant with UK GDPR and data protection standards. Only AI tools vetted and approved by Eton Academy may be used for school purposes.

23.7. Staff must not use AI to process internal strategy, student records, or any content that could lead to data misuse or intellectual property concerns.

23.8. All AI-related incidents — including misuse, data breaches, or inappropriate content — must be reported immediately to the DSL or Senior Leadership Team.

23.9. Disciplinary action may be taken in line with our Staff Code of Conduct and Acceptable Use policies if AI tools are used inappropriately.

Policy Approved and signed by

Eton Academy

Dr Gabrielle Hargreaves
Principal
04/07/25

Appendix 1 - Student Acceptable Use Agreement (Grades 3-6)
Being Safe Online:

1. Our teachers will check how we use computers/email/LMS to keep us safe.
2. I will keep my password secret and won't use someone else's.
3. I'll be careful when talking to people online and won't share personal information like where I live or my phone number.
4. If I see something strange or uncomfortable online, I will tell a teacher or an adult.
5. I won't send or keep mean messages or pictures.

Being Nice Online:

6. I'll respect others and their work. I won't look at or change their work without permission.
7. I will use polite words online and won't use bad words.
8. I understand everyone has different ideas, and I'll be respectful. If someone is mean online, I'll tell an adult.
9. I will speak to students and staff in a respectful way.

Using Computers Right:

10. I'll only use my school email for talking to teachers and school stuff.
11. I won't try to look at or share things that are not okay. I won't try to get around the school's safety rules.
12. If I get a weird email, I won't open any links or attachments unless my teacher says it's okay.
13. If someone sends me a mean email, I'll tell a teacher.

Learning Online:

14. When I find information online, I'll make sure it's true.
15. I'll ask before using someone else's work for my school projects.
16. I won't download music or videos if they're not free.

Remember, I Represent My School:

17. If I do something not okay online, even when I'm not at school, it can still be a problem.
18. If I don't follow these rules, I might not be allowed back to school for a while.

Name:	
Grade:	
Signature:	
Date:	

Appendix 1 - Student Acceptable Use Agreement (Grades 7+)

For my safety:

1. I understand that the school will monitor my use of the IT systems, including the school platform, e-mail, school social media and other digital communications.
2. I will not tell anyone my password nor will I try to use any other person's username and password.
3. I will be aware of 'stranger danger' when I am communicating online.
4. I will not give out any personal information (e.g. home address and telephone number) about myself or anyone else when online.
5. I will not arrange to meet people offline that I have communicated with online.
6. I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
7. I will not store, send or share content of an inappropriate nature, e.g. sexual content, offensive or discriminatory content.

Acting as I expect others to behave toward me:

8. I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
9. I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language (e.g. swear words).
10. I appreciate that others may have different opinions and will respect their right to share their opinions, unless these are offensive or discriminatory, in which case I will report my concerns to a trusted adult.
11. I will not take or distribute images of anyone without their permission.

Keeping secure and safe when using technology in school:

12. I will only use school email for school-related matters, e.g. to contact teachers or other members of staff outside of regular lessons.
13. I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
14. I will not open any attachments to emails unless given permission to do so and I know and trust the person/organisation that sent the email.
15. I will immediately tell a staff member if I receive an offensive email or message, or if offensive content is shared with me.

Using the internet for research or recreation:

16. When I am using the internet to find information, I should take care to check that the information that I

access is accurate.

17. I should ensure that I have permission to use the original work of others in my work.
18. Where work is protected by copyright, I will not try to download copies (including music and videos).

Taking responsibility for my actions, both in and out of school:

19. I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, even when I am out of school, as I recognise I am part of the school community (e.g. cyberbullying, inappropriate use of images and/or personal information).
20. I understand that if I break these rules, I will be subject to disciplinary action as outlined in the school's Behaviour Policy. This may also include loss of access to the school platform.
21. I have read and understood the above and agree to follow the rules outlined.

Name:	
Grade:	
Signature:	
Date:	

Appendix 2 - Parent/Carer Acceptable Use Agreement

The school seeks to ensure that students have opportunities to communicate with one another and their teachers, and to use digital technology to enhance their learning. We expect students to agree to be responsible users. A copy of the Student Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Acceptance of Use Form

Parent/Carer's Name:	
Student's Name:	

As the parent/carer of the above student, I know that my child has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of IT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the school systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies. I understand that recording of lessons should only be made by Eton Academy, and the recording of any classes violates GDPR and privacy policies in the UK. This includes screen recording, recording on other devices and taking pictures of live classes.

I understand that my child's activity on the school systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt the safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signature:	
Date:	

Appendix 3 - Staff Laptop/Devices Acceptable Use Agreement

Acceptable Use

1. This agreement applies to all laptops and other associated devices which are loaned to staff and therefore remain the property of the school.
2. It should be read in conjunction with the school's e-Safety Policy
3. All recipients and users of these devices should read and sign the agreement.
4. All members of staff should recognise that they must only use school IT equipment for schoolwork; they should not use personal IT equipment/devices, email accounts etc, for school matters, and they should not use school equipment for personal matters.

Security of equipment and data

5. The laptop and any other equipment provided should be stored and transported securely. Special care must be taken to protect the laptop and any other devices from loss, theft or damage. Users must be able to demonstrate that they took reasonable care to avoid damage or loss.
6. Staff should understand the limitations of the school's insurance cover.
7. Government and school policies regarding appropriate use, data protection, information security, computer misuse and health and safety must be adhered to. It is the user's responsibility to ensure that access to all sensitive information is controlled.

Software

8. Any additional software loaded onto the laptop should be in connection with the work of the school. No personal software should be loaded.
9. Only software for which the school has an appropriate licence may be loaded onto the laptop. Illegal reproduction of software is subject to civil damages and criminal penalties.
10. Users should not attempt to make changes to the software and settings that might adversely affect its use.

Faults

11. In the event of a problem with the computer, the school's IT support team should be contacted immediately.

Declaration:

12. I have read and understood the above and also the school's e-Safety Policy and agree to abide by the rules and requirements outlined.

Name:	
Signature:	
Date:	

Appendix 4 - Staff Acceptable Use Agreement

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct. Members of staff should consult the school's e-Safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I understand that school information systems may not be used for private purposes.
- I understand that my use of school systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will respect system security, and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware unless authorised to do so.
- I will ensure that personal data, particularly that of students, is stored securely through encryption and password and is used appropriately, following the school e-Safety policy.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with students (including e-mail, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that student use of the internet is consistent with the school's e-Safety Policy.
- When working with students, I will carefully monitor and scrutinise what students are accessing on the internet, as far as is possible when working remotely.
- I know what to do if offensive or inappropriate materials are found, e.g. through file or screen sharing.
- I will report any incidents of concern regarding students' safety to the appropriate person, e.g. DSL.
- The school may exercise its right to monitor the use of the school's systems, including the interception of e-mail and the deletion of inappropriate materials where it believes the unauthorised use of the school's system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

Name:	
Signature:	
Date:	