AYLESBURY GRAMMAR SCHOOL

Founded 1598

ONLINE SAFETY POLICY

This policy is reviewed and updated annually.

This version was approved by the Full Governing Body in January 2023.

The next update will be due by January 2024.

SIGNED: RJ Williams

Richard Williams (Chair of Governors)

AYLESBURY
GRAMMAR SCHOOL
Founded 1598

ONLINE SAFETY POLICY

1. Introduction

1.1 At Aylesbury Grammar School we use technology and the Internet extensively across all areas of the curriculum and as such safeguarding and applying appropriate controls/restrictions are absolutely essential. Online safeguarding is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an online safety incident, whichever is sooner.

1.2 The primary purposes of this policy are:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any potential harm to students or liability to the school.

2. Policy Governance (Roles & Responsibilities)

2.1 Governing Body

The governing body is accountable for ensuring that Aylesbury Grammar School has effective policies and procedures in place and as such they will:

- Review this policy at least annually and in response to any online safety incident
- Ensure that the policy is up to date and covers all aspects of technology use within the school
- Ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those
- Receive updates from the Headmaster with regards to training, identified risks and any incidents

2.2 Headmaster

Reporting to the governing body, the Headmaster has overall responsibility for online safety within the school. The day-to-day management of this will be delegated to a member of staff (online safety officer) as indicated below.

The Headmaster will ensure that:

- Online safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated online safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All online safety incidents are dealt with promptly and appropriately.

2.3 Online Safety Officer

The designated Online Safety Officer is: Mr P Carson, ICT Leader

The online safety officer will liaise in the first instance with:

Mr M Sturgeon, Headmaster
Mrs P Venning, Deputy Head (Designated Safeguarding Lead)
Mr I Digby, Finance & Resources Director (SLT Link for IT Strategy and Development)
Mr G Singh, Assistant Head (SLT Link for Digital Learning)

The Online Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use
- Review this policy regularly and bring any matters to the attention of the Headmaster
- Advise the Headmaster and Governing body on all online safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home
- Liaise with IT technical support and other agencies as required.
- Retain responsibility for the online safety incident log; ensure staff know what to report and ensure the appropriate audit trail
- Ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose
- Make him/herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Headmaster and Governing body to decide on what reports may be appropriate for viewing

2.4 And with support from the ICT Technicians will:

- Ensure anti-virus is fit-for-purpose, up to date and applied to all capable devices
- Ensure software updates are regularly monitored and devices updated as appropriate
- Ensure that any online safety technical solutions such as Internet filtering are operating correctly and have been applied correctly
- Passwords are applied correctly to all users. (AGS recommends that passwords for staff will be a minimum of 14 characters)
- Ensure the ICT System Administrator password is changed on a regular basis.

2.5 Teaching and Support Staff

All staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headmaster.
- Any online safety incident is reported to the online safety Officer (and an online safety Incident report is made), or in his/her absence to the Headmaster. If you are unsure the matter is to be raised with the online safety Officer or the Headmaster to make a decision.

2.6 Students

- The boundaries of use of ICT equipment and services in this school are given in the ICT Acceptable Use Policy for Students
- Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the school behaviour policy
- Online safety is embedded into the curriculum - students will be given the appropriate advice and guidance by staff, in all subject areas across the curriculum
- All students will be fully aware how they can report areas of concern whilst at school or home, for example issues concerning online bullying or sexting (YPSI - Youth Produced Sexual Imagery) This is also detailed in the Acceptable Use Policy for Students

2.7 Parents/Carers

Parents play the most important role in the development of their children and as such the school will ensure that parents have access to resources to acquire the skills and knowledge they need to ensure the safety of children outside the school environment.

2.8 Through parent information evenings, school newsletters and the availability of free online training courses (Think U Know) the school will keep parents up to date with new and emerging online safety risks and will involve parents in strategies to ensure that students are empowered.

2.9 Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such all new parents will be asked to read and agree to the ICT Acceptable Use Policy for Students before their child can be granted any access to school network, ICT equipment or services.

3. Network and Device Management

3.1 Aylesbury Grammar School uses a range of devices including desktop PCs, laptops, chromebooks and tablets. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

3.2 Internet Filtering

We use several layers of filtering to minimise access to illegal and inappropriate websites. The ICT Leader (Online safety officer) and IT Technicians are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headmaster.

3.3 Internet Filtering on BYOD Chromebooks

Every BYOD Chromebook managed by the school will install Senso (senso.cloud) when a student logs in to their AGS account. If the student is logged into their AGS account at home, all web filter rules that apply in school will also apply at home. If parents do not want their child to be subject to the school's web filtering at home, then they should log in with their personal account. If parents would like to apply their own filtering/monitoring/screen time rules to their child's personal Google account, then they should use Google Family Link. Family Link will allow parents to set up monitoring on their child's account.

3.4 Email Filtering

We use Microsoft Office 365 which provides filtering to minimise the amount of infected email received. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. The system is also used to filter certain words and can be used for monitoring.

3.5 Passwords

All staff and students will be unable to access the network without a unique username and password. Staff and student passwords should be changed if there is a suspicion that it has been compromised. The ICT Leader will be responsible for ensuring that passwords are changed as and when required.

3.6 Anti-Virus

All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headmaster if there are any concerns.

4. Email

4.1 All school employees and students are issued with a school email account, the address ending with; @ags.bucks.sch.uk

4.2 All staff are reminded that emails are subject to *Freedom of Information and **Subject access requests, and as such the email service is expected to be used for professional work-based emails only. The use of personal email addresses for the purposes of contacting students is not permitted.

4.3 Students are permitted to use the school email system too, and as such are all issued with an AGS email account and their own approved email address. Students should use this email account only for school-based activity as laid out in the student Acceptable Use Policy that they have signed on entry to the school.

* Freedom of Information Act - https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

**A Subject Access Request is a written, signed request from an individual to see information held on them. The Data Controller must provide all such information in a readable form within 1 month of receipt of the request and may charge a small fee (up to £10).

5. Photos and videos

5.1 A photo release statement is agreed to by parents/carers as part of the school admissions pack upon a students' entry to the school. A list of students who are not permitted to be photographed will be available to all staff with reminders sent out periodically. This list will also be kept by the online safety officer and where relevant the school's designated safeguarding lead.

5.2 Students may **not** take photos or video footage for personal use anywhere on the school site unless they have permission from the Headmaster or any other member of the Senior Leadership Team (SLT). Students must ensure that any photos or video footage created under these agreed terms do not bring the school into disrepute in any way. Any photos or video footage taken in lessons (to enhance a practical activity etc.) must be deleted once their purpose has been fulfilled.

5.3 For any photos or video footage used by the school for promotion or celebration purposes there should be no identification of individual students using first name and surname unless specific prior consent has been given. An individual's first name only is to be used, if at all.

6. Social Networking

6.1 Aylesbury Grammar School is fully supportive of social networking as a tool to engage and collaborate with learners, parents and the wider school community. Any use of social media services in school must be in accordance with the 'ICT Acceptable Use Policy for Staff' which includes a Social Media Appendix.

7. Copyright

7.1 Should it be brought to the school's attention that there is a resource which has been inadvertently uploaded, either to the school website or school/department authorised social networking sites, and the school does not have copyright permission to use that resource, it will be removed within one working day.

8. Reporting online safety Incidents

8.1 Any online safety incidents must be brought to the immediate attention of the online safety officer, or in his/her absence the Headmaster. The online safety officer will assist in taking the appropriate action to deal with the incident, liaise closely with the relevant school pastoral teams to ensure the appropriate resolution of the incident and to complete and maintain an incident log.

8.2 All staff should make themselves aware of the procedures and the responsible staff involved in the process.

9. Training & Curriculum

9.1 It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues, and the regular distribution of online safety information to staff, students and parents/carers.

9.2 The school will ensure that aspects of online safety for students is firmly embedded into the curriculum. All students in Years 7-11 complete online safety training, updated periodically. A similar training module is completed by all teaching staff and governors every three years and is similarly offered to parents too.

9.3 Whenever ICT is used in school, staff will ensure that students are made aware of the safe use of technology and risks as part of the students' learning and understanding. Heads of Department should be able to demonstrate where and how the awareness of risk is imparted to students in lessons.

10. Monitoring and Review

10.1 This policy will be reviewed and approved annually by the school's SLT and Governing Body

APPENDIX 1

ONLINE LESSON/MEETING PROTOCOLS

1. Online lessons or meetings should only be used for groups of students except in the following agreed circumstances and only following receipt of written consent from a parent/carer:

   - Foreign Language teachers conducting speaking exercises where group conversations are not conducive to the overall learning or exam preparation
   - Pastoral leaders (SLT, Heads of Year and Heads of House) where a face to face conversation is necessary for the positive welfare of the student involved

2. All participants in the online lesson or meeting should be appropriately dressed and sat up. Participants should not be located in bedrooms (although for students this may be the only suitable place for them to be located, so it is permissible as long as they are appropriately dressed and sat up)

3. Online lessons or meetings must be recorded, by staff, for safeguarding purposes.

4. Students do not have to use their camera if they are reluctant or uncomfortable to do so but they should be encouraged by staff to do so.

5. Participants should be situated in front of a plain/neutral wall or background, with no personal details or offensive/inappropriate material displayed at any time.