AYLESBURY GRAMMAR SCHOOL

E-SAFETY POLICY

1. Introduction

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 (E-Safety), is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

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)

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 e-safety incident
- Ensure that the policy is up to date and covers all aspects of technology use within the school
- Ensure e-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

Headmaster

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

The Headmaster will ensure that:

- E-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 e-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

E-Safety Officer

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

The e-Safety officer will liaise in the first instance with:
Mr M Sturgeon, Headmaster
Mrs P Venning, Deputy Head (Designated Safeguarding Lead)
Mr G Dallas, Assistant Head (SLT Link for ICT Development)

The e-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, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home
- Liaise with IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail
- Ensure any technical e-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 e-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

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 e-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 8 characters with uppercase and numbers included)
- Ensure the ICT System Administrator password is changed on a regular basis.

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 e-safety incident is reported to the e-safety Officer (and an e-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 e-safety Officer or the Headmaster to make a decision.

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
- E-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

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.

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 e-safety risks, and will involve parents in strategies to ensure that students are empowered.

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 Year7 parents will sign the ICT Acceptable Use Policy for Students before their son can be granted any access to school network, ICT equipment or services.

3. Network and Device Management

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

- Internet Filtering

We use a web filter that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites. The ICT Leader (E-Safety Officer) and ICT Technicians are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headmaster.

- Email Filtering

We use Microsoft Office 365 which prevents any infected email to be sent from the school, or to be received by the school. 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.

- 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.

- 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

All school employees and students are issued with a school email account, the address ending with;

@ags.bucks.sch.uk

All staff are reminded that emails are subject to Freedom of Information 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.

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.

5. Photos and videos

A photo release slip is signed by parents as part of the Home/School agreement on 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 e-safety officer and where relevant the school's child protection (CP) Officer.

Students may not take photos or video footage for personal use anywhere on the school site unless they have written permission from the Headmaster. Any photos or video footage taken in lessons (to enhance a practical activity etc.) must be deleted once their purpose has been fulfilled.

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. An individual's first name only is to be used, if at all.

6. Social Networking

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

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 E-safety Incidents

Any e-safety incident must be brought to the immediate attention of the e-safety officer, or in his/her absence the Headmaster. The e-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.

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

9. Training & Curriculum

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 e-safety information to staff, students and parents/carers.

The school will ensure that aspects of e-safety for students is firmly embedded into the curriculum. All students in Years 7-11 complete an online safety training module which is updated annually. A similar training module is completed by all teaching staff annually and bi-annually by governors and parents.

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.

March 2016