



ONLINE SAFETY POLICY

In addition to the AHS Safety Policy which aims to provide for the physical safety of pupils and staff, our Online Safety Policy aims to provide for the safety of pupils and staff when using the digital network.

At Alexandra House School we are very aware of the benefits of using modern technology to enhance learning both in school and at home but we are also acutely aware of the serious dangers to children which can be caused by incorrect use of these tools. We believe that children of primary school age need to be protected against the dangers while using the internet and that they deserve to enjoy their childhood for as long as possible, free from long periods of watching a screen. We encourage them to appreciate the joy of reading books and outdoor play and believe that too much screen time is putting the art of human conversation and interaction in danger. While access to online information can be highly educational, we believe that too much time spent online is ultimately damaging. Therefore, we aim for a balanced use of technology and online resources for educational purposes while keeping a close eye on the children's safety.

We limit the pupils' activity to using the internet for doing web searches for educational purposes and using emails for communication. We do not allow the pupils to use social networking sites such as Instagram, Facebook, Twitter, etc. We strongly discourage parents from allowing their children to have unsupervised access to the internet and to social networking sites out of school also and suggest that all parents take a look at the Gooseberry Planet website which gives details of many of the dangers inherent in using these media and of how to reduce these dangers.

Being a small school, it is relatively easy for us to monitor online usage. We therefore have strict controls in place in order to provide access while minimising the dangers.

Access while in school

Each classroom, as well as the multi-purpose hall, is equipped with a whiteboard, projector and laptop. The computer room has six laptops for the children's use. All of these are connected to the internet.

Safety Measures

The internet access is protected by a password, which is issued only to teachers and never given to the children. Pupils are never given access to the computers without the teacher being present, and it is the teacher who switches on and off the equipment and the internet access at all times. When doing research, pupils are given specific safe sites to use. The computer room is set up in such a way as to ensure that the teacher can see all the screens which the children are using, thereby being able to monitor the content at all times. In class, the teacher always monitors the pupils' use of all electronic equipment also.

Personal mobile phones

We realise that some parents may wish their children to bring a mobile phone to school with them so that they may contact them if necessary during the trip to and from school. However, they must agree to the following limitations on its use:

Mobile phones must be switched off and placed in a bag on arrival at school.

- The phone must be kept out of sight and not used in the building and school grounds.
- The security of the phone will remain the pupil's responsibility.
- If a pupil is found using a mobile phone in school it will be confiscated by a member of staff and may be collected from the Headmistress at the end of the school day.
- In the case of repeated use of a mobile phone, the phone will only be returned to a parent who will be required to visit the school by appointment to recuperate same.
- If asked to do so, content on the phone (e.g. messages, emails, pictures, videos, sound files) will be shown to a teacher.

Please also see Electronic Devices – Search and deletion policy.

If children need to contact their parents by phone during the school day for a good reason, they may ask the teacher/secretary for permission and will be allowed to use the school phone for this purpose.

Implementation of the Online Safety Policy

All teachers are responsible for promoting and supporting safe behaviours in the use of ICT. We encourage pupils to feel able to report any bullying, abuse or inappropriate materials they may find online.

All AHS staff are made aware of the school's expectations with regard to:

- The safe use of email
- The safe use of internet
- The safe use of school network, equipment and data
- The safe use of digital images and digital technology
- Their role in providing safety education for pupils

How Staff, Parents and Pupils will be informed of these Procedures

- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'
- Upon admission, Parents' Permission Form for ICT (Appendix 1) is to be signed for all pupils
- Upon admission, Parents' Permission Form for Use of digital videos/images (Appendix 2) is to be signed for all pupils

- Upon admission, an Acceptable Use of ICT Agreement (Appendix 3a or 3b) is to be signed by all pupils and a parent
- All staff will be required to sign the school's Online Acceptable Use Agreement (Appendix 4)

(Please see all appendices at the end of this document)

Managing Email Safety

Email is now an essential means of communication for staff and pupils at Alexandra House School and at home. Directed email use brings significant educational benefits through increased ease of communication between pupils and staff, or within local and international school projects. Alexandra House School reserves the right to monitor email to provide a safer email environment for pupils.

Pupils are made aware of the risks and issues associated with communicating through email and the strategies to deal with inappropriate emails as part of the school's Online Safety education programme.

Pupils are taught about the safety and 'etiquette' of using email i.e.

- Not to give out their email address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer
- That an email message should be clear, short and concise
- That any email sent should be written carefully and authorised before sending
- They must not reveal private details of themselves or others in email, such as address, telephone number, etc
- To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe
- That they must immediately tell a teacher/responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature
- Not to respond to malicious or threatening messages and emails but to keep and report them as evidence
- Not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them
- That forwarding 'chain' email letters is not permitted

Managing Digital Images and Video Safely

The AHS website is an important, public facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it is an effective way to share the school's good practice and promote its work.

A senior member of staff oversees and authorises the website's content and checks suitability. When uploading digital images or video AHS follows the following practice:

- Pupils are not named

- Parental permission is obtained upon admission to AHS for publishing any photographs or video footage of pupils on the school website or in a newsletter or message (See Appendix 2)

Using the school equipment, network and data safely

The computer system and network is owned by the School and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The School reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet or email activity on the network.

Online Safety Infringements and Sanctions

Alexandra House School will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The School cannot accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counseling by Head of School
- Informing parents
- Removal of Internet or computer access for a period
- Suspension

Our ICT and E-Learning teachers act as first point of contact for any infringements. Any complaint about staff misuse is referred to the Head of School. Complaints related to child protection are dealt with in accordance with school child protection procedures.

In extreme cases the school reserves the right to search pupils for 'banned items' and 'delete data' stored on seized device (See Electronic Devices – Searching and Deletion Policy).

Electronic Devices – Searching & Deletion Policy

Introduction

The changing face of information technologies and ever increasing pupil use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. One particular change is the power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

The items banned under school rules are as follows:

- Mobile phones
- Personal computers and laptops
- Tablets

These items can be searched for by an authorised member of staff with or without the permission of the pupil.

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

Responsibilities

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation.

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data/files on those devices:

- ICT Teacher
- All class teachers
- All subject teachers

Training/Awareness

All members of staff are aware of the school's policy on "Electronic devices – searching and deletion". The members of staff that are authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data/files from those devices will inform the Headteacher and will carry out deletion in her presence.

Electronic Devices

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material (if it poses a risk to the physical or mental harm of a child), retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. A record will be kept of the reasons for the deletion of data/files.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain it, they may erase any data or files, if they think there is a good reason to do so.

Care of Confiscated Devices

School staff are reminded of the need to ensure the safekeeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices (particularly given the possible high value of some of these devices).

Audit/Monitoring/Reporting/Review

The Headmistress will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data/files using the Online Safety Incident Log.

These records will be reviewed by the Directors at regular intervals.

This policy will be reviewed by the Headmistress and directors annually and in response to changes in guidance and evidence gained from the records.