ALDENHAM
FOUNDATION

Online Safety Policy

January 2026 by
Head of Technology (JC)

Scope

This policy applies to all members of the Aldenham Foundation who have access to and are users of the Foundation IT systems (including staff and pupils). In this policy 'staff' includes teaching and operational staff, governors, and volunteers.

This policy covers both fixed and mobile internet devices provided by the Foundation (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.) as well as all devices owned by pupils or staff and brought onto School premises (personal laptops, tablets, smart phones, watches etc).

Online Communications

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. IT and online communications can greatly enhance learning, but also pose risk.

Current and emerging technologies used in and outside of school include:

- Websites
- Email and instant messaging
- Blogs
- Social networking sites, chat rooms
- Music / video downloads
- Gaming sites, virtual-reality and augmented-reality devices and games
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as smart phones and tablets.
- AI

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

We understand the responsibility to educate our pupils on online safety issues, to teach them the appropriate behaviours and critical-thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety.

The Foundation:

- Regularly reviews the methods used to identify, assess and minimise online risk;
- Examines emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted;
- Ensures that appropriate filtering and monitoring is in place and take all reasonable

precautions;
- Puts measures in place to ensure that users can only access appropriate material.

This policy, supported by the Acceptable Use of ICT Policy for staff and pupils, is implemented to protect the interests and safety of the Foundation including boarders. It aims to provide clear guidance on how to minimise risks. It is linked to the following policies:

- Safeguarding Policy;
- Staff Code of Conduct;
- Health and Safety Policy;
- Behaviour Policies;
- Anti-Bullying Policy;
- Acceptable Use of ICT Policies (staff and pupils);
- Social Media Policy; and
- Data Protection Policy

Roles & Responsibilities

In line with *Keeping Children Safe in Education (2025)*, each school's Designated Safeguarding Lead (DSL) has overall responsibility for online safety. The Head of Technology works closely with the DSLs to ensure that:

- Staff are adequately trained about online safety; and
- Staff are aware of the Foundation procedures that should be followed in the event of breach or suspected breaches of online safety.

The Head of Technology works with the Bursar to ensure that this policy is understood and upheld by all members of the Foundation and to help the Schools keep up-to-date with current online safety issues and guidance issued by relevant organisations, including the Independent Schools Inspectorate, Social Services, CEOP (Child Exploitation and Online Protection) and Childnet International. All safeguarding issues must be raised with the DSL.

The IT Department has a key role in maintaining a safe technical infrastructure at the Foundation and in keeping abreast with technical developments. They are responsible for the security of the Foundation's hardware system, its data and for training the Foundation's teaching and administrative staff in the use of IT. They will monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the Head of Technology.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the Foundation's online safety procedures.

If the School believes that a child or young person is at risk as a consequence of online activity, it may seek assistance from CEOP (Child Exploitation and Online Protection).

Pupils from Year 3 upwards are responsible for using the Foundation's IT systems in accordance with the ICT Acceptable Use Policy, and for letting staff know if they see those systems being misused.

It is essential for parents to be fully involved in the promotion of online safety, both in and outside of school. We regularly consult and discuss online safety with parents.

Staff

All staff are required to have read and accepted the ICT Acceptable Use Policy before accessing the Foundation's systems (usually via the induction process). New staff receive information on Aldenham Foundation's Online Safety, Acceptable Use and Social Media Policies as part of their

induction.

All staff receive regular information and training on online safety issues in the form of INSET training and internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise.

Duty to Report Online Safety Breaches and Safeguarding Concerns

Staff should promptly inform the Head of Technology if they suspect or become aware of an online safety breach, except where the case involves safeguarding concerns, in which case the matter should be reported as set out below:

- Staff must promptly inform the Designated Safeguarding Lead (preferably via CPOMS) if they have any safeguarding concerns about a pupil related to online activity (including sexting, cyberbullying and inappropriate or illegal content). The DSL will liaise with the Deputy Head (Pastoral) about an appropriate course of action to take upon receipt of the notification.
- Where appropriate, safeguarding concerns will be reported to relevant agencies (which may include social services, the police and CEOP).

Online Safety in the Curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for online safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

Pupils throughout the Foundation are taught about safety matters through the Informatics curriculum. In addition, the Foundation provides opportunities to teach about online safety within a range of curriculum areas. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, and usually via Wellbeing, pupils are taught about how to look after their own online safety, about recognising online sexual exploitation, stalking and grooming, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to any member of staff at their respective Schools in accordance with the Safeguarding Policy. Pupils can also contact Childline or the Children's Commissioner.

At age-appropriate levels, pupils are also taught about relevant laws applicable to using the internet, such as data protection and intellectual property. All pupils are taught about respecting other people's information and images.

Pupils are taught about the impact of cyber-bullying and how to seek help if they are affected by it.

Pupils should approach any member of staff for advice or help if they experience problems.

Staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, pupils need to recognise the risks attached to publishing their own images on the internet (eg. on social networking sites).

Guidance for Parents

The Foundation seeks to work closely with parents in promoting a culture of online safety. The respective Schools will always contact parents if it has any concerns about pupils' behaviour in this area and encourages parents to share any concerns with the School.

The Foundation will provide information and guidance on online safety by a variety of means (including offering specific online safety guidance at parent forums and other events).

Foundation Email Accounts

Staff and pupils should immediately report to the Head of Technology (or in the case of pupils, their form tutor) the receipt of any communication that makes them feel uncomfortable or which is offensive, discriminatory, threatening or bullying in nature. They should not respond to any such communication.

Email communications through the Foundation network, Wi-Fi and staff email accounts are monitored.

Use of the Internet and Social Media

The Foundation expects pupils and staff to think carefully before they post any information online or repost or endorse content created by other people.

Staff and pupils should ensure their online communications do not:

- Place a child or young person at risk of or cause harm;
- Breach confidentiality;
- Breach copyright or data protection legislation; or,
- Discriminate against, threaten, bully or harass any individual.

Certain websites are automatically blocked by the Foundation's filtering system. If this causes problems for schoolwork / research purposes, pupils should contact their form tutor for assistance. Pupils should report to their Form Tutor if they accidentally access materials of a violent or sexual nature whilst using Foundation's equipment.

All internet usage via the Foundation's systems and its network is monitored. Deliberate access to inappropriate material may lead to disciplinary action.

Staff should also refer to the relevant Staff Code of Conduct and the Social Media Policy.