Dame Alice Owen's School
The Dame Alice Owen Foundation – 1613

INFORMATION TECHNOLOGY AND ONLINE SAFETY POLICY

Agreed by the Governing Body School Community Committee	February 2026
To be reviewed	Spring 2028
(reviewed every 2 years)	

To be monitored by the Deputy Headteacher, Designated Safeguarding Lead, Director of Digital Technology and the Governing Body School Community Committee

1. Aim

To equip students for the modern world by helping students to:

- develop knowledge and skills to use computers effectively
- understand how they can keep themselves safe online
- develop effective learning strategies to become an autonomous user of Information Technology.

To support all members of the school community in their roles by:

- promoting and supporting the use of Information Technology in all areas of the school
- ensuring all members of the school community understand how to keep themselves and others safe online
- providing and making use of online platforms to enable students and teachers to collaborate using a 21st Century toolset
- making full use of Information Technology for collaboration on projects
- using technology to facilitate efficient working practices.

2. Digital Literacy and online safety in the Curriculum

Digital Literacy is a term now used to describe a skillset and knowledge base which enables members of our school community to use Information Technology efficiently and safely.

For students, this is mainly delivered through Computer Science lessons and Physical, Social, Health, Relationship and Sex Education (PSHRSE) known as Learning for Life (L4L).

The objectives of the digital literacy curriculum regarding online safety are to enable students to use Information Technology appropriately to:

- build confidence in their use of Information Technology beyond activities familiar to them such as social media and gaming
- enable students to consider, discuss and evaluate the implications of using Information Technology in everyday life.
- help students to understand how they use technology safely and responsibly and how to get help when things go wrong.

We believe it is essential for online safety guidance to be given to the students on a regular and meaningful basis. Online safety is embedded within our curriculum and we continually look for new opportunities to promote online safety.

- The School has a framework for teaching internet skills and online safety in Computing lessons in Key Stage 3 and through the L4L sessions in Years 7-11.
- Educating students about the online risks that they may encounter e.g. How to evaluate the truth of what they see online, acceptable and unacceptable online behaviours, how to identify online risks and how and when to seek support, takes place during specific L4L sessions. Assemblies and informal opportunities are also used to reinforce online safety.
- Students are taught about the relevant legislation when using the Internet, such as data protection and intellectual property.
- Students are taught about copyright, respecting other people's information, safe use of images, consent and other important areas through discussion, modelling and appropriate activities.
- Students are taught the impact of online behaviour and know how to seek help if they are affected by any form of online bullying or if they have posted something they regret. Students are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher or trusted staff member, or an organisation such as Cybermentors, Childline or the Child Exploitation and Online Protection Centre (CEOP) report abuse button.
- Students are aware of the Reporting Concerns page on the Student Launchpad which allows students (anonymously if they wish) to give the pastoral team any information about online behaviour. This is then monitored daily during term time by the pastoral team. Students are also told they can report issues directly to the pastoral team, or can contact Childline or the NSPCC.
- Students are taught critically to evaluate materials and learn good online searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

3. Staff professional Development in the use of Information Technology

The Senior Leadership Team (SLT) together with advice from the Director of Digital Technology establish training needs priorities. The Director of Digital Technology leads the

Information Technology Curriculum Group who meet regularly to discuss updates, plans and training needs of teaching staff; all departments are invited to send a representative to this group.

Information Technology training is carried out through:

- buying in external providers
- Twilight CPD sessions
- Staff meetings and briefing
- Personal CPD and sharing of good practice amongst colleagues.

4. Online safety skills development for staff

Our staff receive appropriate information and training on online safety through staff meetings, Inset and briefings. New staff receive information on the school's acceptable use policy as part of their induction.

All staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community. All staff are encouraged to incorporate online safety activities and awareness within their curriculum areas, including helping students to understand the benefits and drawbacks of AI.

5. A Supportive e-Community – Our approach to online safety

At Dame Alice Owen's, we seek to establish a supportive community, and this extends to online communications as well as telephone conversations and face to face meetings. Our approach is restorative. Where issues arise, we seek to support students in:

- Changing their online behaviours where necessary
- Removing/ undoing any online record of their activity and addressing their online digital footprint
- Addressing any relationship issues that have arisen from their activity

Where appropriate, sanctions are used, but the focus remains on helping the student to learn and move forward in their behaviour.

6. Online safety - Roles and Responsibilities

Online safety is an important aspect of school life.

The named Online Safety Coordinator in this school is Colin Jackson. Under the oversight of the Designated Safeguarding Lead, and with the support of the Pastoral Directors, the Online Safety Coordinator's role is to keep abreast of current online safety issues and relevant guidance from the DfE and other local and national bodies. The Senior Leadership Team and Governing Body are updated by the Headteacher/Online Safety coordinator at least annually through the Headteacher's report. The Governing Body understands the issues and strategies at Dame Alice Owen's School in relation to local and national guidelines and advice.

This policy, supported by the School's Acceptable Use Policy for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to other policies as follows: Safeguarding and Child Protection, Health and Safety, Positive Behaviour and Anti-bullying and Safe Use of Images policies. All of these policies are available on the school website.

7. Managing the School online safety Messages

We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used. The key online safety advice is promoted widely through Learning 4 Life lessons, school displays, newsletters, class activities, assemblies etc.

8. Involving parents/carers

Parents and carers are invited to online safety evenings so that they are aware of the School's approach to these issues and also to give them advice on what they can do to keep their children safe online. These evenings also serve to keep them as up to date as possible of the online environment the children experience.

Wherever appropriate, issues are shared with families so that home and school can work together in establishing a supportive e-Community.

9. Incident Reporting, online safety Incident Log & Infringements

All online safety concerns or issues are reported as soon as practically possible to the relevant Pastoral Manager/Director, or to the Designated Safeguarding Lead if there is an immediate safeguarding concern. The School uses software to monitor and filter student and staff usage of our IT system and alerts are triggered when certain keywords or behaviours are typed.

10. Management of Information Technology

The Senior Leadership Team decides the strategic planning of Information Technology in consultation with the Director of Digital Technology and the Network Manager. Separate strategic vision and planning documents provide the framework for an annual Information Technology Development Plan. The progress of this plan is monitored by the Deputy Head and Director of Digital Technology.

11. Access to Information Technology

Staff are supplied with a laptop computer for electronic registration and also for developing and delivering their subject. Staff are also able to access the school network offsite by a variety of methods including use of cloud services and by connecting to the school network by secure methods.

Information Technology facilities are available to departments through a booking system. Departments that require the use of computers for a specific unit of work within their syllabi, can book portable technologies for use in lessons or coordinate with the computing teaching staff and book computer rooms for specific lessons.

Students have access to Information Technology facilities in the Library and in K6 during lunchtimes. Sixth form students can also use the Information Technology facilities in the Self Access Learning Centre (SALC). Student access to technology is supervised at all times, using monitoring software. If students misuse any of the Information Technology facilities then they will be subject to the school rules regarding conduct and school property.

The School has a policy for the use of computing facilities including the Internet. Students and parents sign this policy annually to help clarify expectations - see Appendix 1.

12. Technical Support

The school has a Network Manager and a team who are responsible for ensuring the running of the curriculum network.

Support from outside agencies will be used, as appropriate. It will be our policy to review the staffing requirements based on the nature and quantity of Information Technology changes, providing training and support for the technical support team to ensure new initiatives achieve maximum success.

13. Hardware Resources

A specific yearly sum is allocated for the repair and maintenance of the network. Funds for the development of the network come from external sources.

The identification of hardware needs, and the order of their priorities, is decided by the SLT and the Director of Digital Technology with the Network Manager in consultation with stakeholders in the school community. This list of priorities is included in the Five-Year Information Technology Master Plan.

14. Software Resources

The Network Manager is responsible for the upgrading of network software and its security. The identification and purchasing of and access to software for specific departmental use must be agreed by the Network Manager and the relevant Head of Department. The Network Manager is responsible for the development of the school’s Information Technology infrastructure to ensure the School is able to meet the needs of all members of its community.

Where there are GDPR issues surrounding the software, staff must get approval from the Data Protection Officer, including for the use of websites where student data will be held by a third party.

15. Data Protection Act – Requirements with respect to ‘Fair Processing’

The Data Protection Officer will be responsible for ensuring all necessary compliance documentation is in place and up to date. All students and parents will be made aware of the School’s responsibilities. A letter will be issued to all new students and information will be made available on the school website. Before any new software or web-based products that require sharing of any information is used, the GDPR issues arising must be checked with the Data Protection Officer.

16. Health and Safety

The use of Information Technology conforms to the School policy in this area.

17. Reporting to parents

Reports to parents are sent electronically. Hard copies are available to parents on request.

18. Monitoring

The aspects of Information Technology referred to in this policy will be monitored within departments by the Head of Department and by the Information Technology Curriculum Group. The DSL has lead responsibility for understanding filtering and monitoring and processes in place in school, as well as responding to any safeguarding concerns that arise from these.

Appendix 1

Student IT Agreement

I will:

- Only use school technologies for school-related activities
- Follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline
- Treat school resources carefully, and report issues or faults
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies
- Be cautious to protect the safety of myself and others
- Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online
- Use school technologies at appropriate times, in approved places, for educational pursuits
- Cite sources when using online sites and resources for research
- Recognise that use of school technologies is a privilege and treat it as such
- Help to protect the security of school resources

I will not:

- Use school technologies in a way that could be harmful to myself and others
- Attempt to find inappropriate images or content
- Engage in cyberbullying, harassment, or disrespectful conduct toward others
- Try to find ways to circumvent the school's safety measures and filtering tools
- Use school technologies to send spam or chain mail
- Plagiarise content I find online
- Post personally-identifying information, about myself or others
- Agree to meet someone I meet online in real life
- Use language online that would be unacceptable in the classroom
- Use school technologies for illegal activities or to pursue information on such activities
- Attempt to hack or access sites, servers, or content that isn't intended for my use

You signed this when you joined the school

Student	Parent/Carer
Signed :	Signed :
Print name:	Print name:
Date:	Date:

Staff Acceptable Use Agreement:

Professional responsibilities when using any form of ICT, including the Internet, in school and outside school.

- For your own protection we advise that you:
- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook, Twitter and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your personal details, such as mobile phone number, personal email address or social network details to pupils, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.
- Only take images of pupils and/or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, both in school and outside school, will not bring the school or your professional role into disrepute.
- You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

Protocol for sending emails

Email has become an important and essential means of communication which should help us improve the communications within school. Before sending emails consider the following:

- Does an email need to be sent at all? Would it be better to actually speak to someone at break or lunchtime?
- How will the email look to the recipient? Is the tone what is intended or does it appear very abrupt?
- Subject line should always be completed so staff can see if it is relevant to them or not without having to open the email.
- Is the email likely to be read in time? If a matter is urgent, consider the fact that colleagues may be teaching all day and only check their email at a specific time.

Who does the email need to be sent to?

- Is there a group set up that could be used e.g. If it is for Y9 form tutors, choose that rather than just teaching staff.
- Some sent to teaching staff may only need to be sent to one teacher. If it is about a particular student, use SIMS/Edulink to find the relevant teacher by looking at the student’s timetable and targeting the email accordingly.

- If a student is missing from your lesson and there is no explanation, send an email to the Attendance for them to investigate.
- If people are copied in, why is that being done? Copying in a line manager should not be the automatic action but may be appropriate to aid communication.
- If forwarding emails make sure it is clear to the recipient why you have done this and what response you expect from them.
- Blanket emails should not be used for selling personal items or asking colleagues for sponsorship. Feel free to use the staff bulletin for that.