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

INFORMATION TECHNOLOGY AND ONLINE SAFETY POLICY

Agreed by the Governing Body Curriculum Committee	February 2024
To be reviewed	Spring 2026
(reviewed every 2 years)	

To be monitored by the Deputy Headteacher, Designated Safeguarding Lead, Director of Digital Technology and the Governing Body Curriculum 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 concerns@damealiceowens.herts.sch.uk email address to which they can send (anonymously if they wish) 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.

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. It is the role of the online safety coordinator, with the support of the Pastoral Directors, to keep abreast of current issues and relevant guidance available from the DfE and other local and national bodies.

The Senior Leadership Team and Governing Body are updated by the Head/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, Home – School agreement, 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. Online safety guidance is offered in the school homework diaries. The key online safety advice is promoted widely through 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 is set out and also to give them advice on what they can do to keep their children safe online. These evenings also serve to 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 decide 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, coordinate with the computing teaching staff for use of the computer rooms. The rooms can also be booked for specific lessons. In addition to the computer rooms, subject teachers can book portable technologies for use in lessons.

Students have access to Information Technology facilities in the Library and in K5 during lunchtimes. Sixth form students can also use the Information Technology facilities in the Self Access Learning Centre (SALC) and 6th Form Common Room. 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 the use of websites e.g. 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 using the 'In-touch' feature in SIMS. 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

(text taken from the new student booklet available on the school website)

COMPUTER NETWORK

We have a large complex computer network on which we run Windows 10, plus a variety of software, with Google Workspace and Microsoft Office 2019 being the most widely used across departments. All students and staff are allocated their own computer username and password and a Google workspace username and password. They have their own Google drive to store work on. Computers may be used by them during lunchtime in the Libraries or at Computer Club, as well as in lessons.

Access to the Internet is available throughout the school. Students are expected to use this resource sensibly for study purposes only.

Our computing facilities are extremely good and we try to maintain this level of excellence by continual investment in the equipment. We hope that all students will enjoy using the facilities and find that they become fluent in using the computer as a tool to aid their understanding and to enhance the presentation of their work.

All year groups are allowed to connect their own personal tablet or laptop to the school's wireless system for research and study purposes only. These devices are brought into school at the student's own risk. There are robust filtering and monitoring measures in place for all devices, including phones or tablets, connected to the school internet. These block inappropriate websites and alert the DSL if a student is attempting to access concerning content. Parents/carers are informed of the filtering and monitoring systems in place via the annual Safeguarding letter and Online Safety information evening. It is furthermore made clear to parents via the same means that school systems cannot block or monitor content accessed by students via mobile data and that they play a role in monitoring their children's phone use to ensure students' online safety both in and out of school. Information is shared with parents/carers about how they can achieve this.

Rules for the use of Computers

Students are expected to behave in a quiet and responsible manner and to abide by the following rules:

STUDENTS MUST NOT:

- Use any computer Username other than their own
- Attempt to access any part of the computer or network which they are unauthorised to access which is an offence under the **Computer Misuse Act 1990**
- Load any unauthorised programs on to the network
- Interfere with another student's use of a computer in a way which has a negative effect on their work

- Disconnect or move any piece of equipment attached to a computer, e.g. printer, monitor, keyboard, headphones or mouse
- Print excessively
- Enter a computer room unless accompanied by a member of staff.

ANY problems with computers, printers or any other hardware must be reported to the IT Support Team.

Staff and students must take reasonable care to protect data held on school IT systems.

Students should log off when they finish using a computer for the safety of their own data. Any waste paper should be put in the recycling (blue) boxes or in the bin.

No food, drink or chewing gum to be brought into or consumed in computer rooms.

Students are responsible for the security of their password and should not share it with anyone.

When in class, access to the Internet is only allowed to assist with school work.

Any unsuitable sites found by accident must be reported immediately to the Network Manager for filtering out.

If students transfer their work to and from home on a memory stick or by e-mail then their home computer must have an up to date virus protection program installed on it.