



PURPLE OAKS ACADEMY

Purple Oaks Academy

Online Safety Policy

E Safety Lead	Mrs Helena Bull	hbull@purpleoaksacademy.org
DSL	Mrs Helena Bull	hbull@purpleoaksacademy.org
Created:	1/09/25	
Review Date:	1/09/26	

Table of Contents:

Policy Statement.....	3
Policy Governance (Roles & Responsibilities)	3
Online Safety Lead.....	3
IT Technical Support Staff.....	4
Teaching and Associate Staff.....	4
All Students.....	4
Parents and Carers	5
Network and Device Management	5
Reporting E-safety Incidents	7
Training and Curriculum	7

Policy Statement

E-safety may be described as the school's ability to protect and educate students and staff in their use of technology and to have the mechanisms in place to intervene and support any incident where appropriate.

At Purple Oaks Academy we recognise the benefits of technology and the internet in supporting students in their education and we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as 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 purpose of this policy is twofold:

- 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 foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Purple Oaks Academy website.

Policy Governance (Roles & Responsibilities)

The Principal and Deputy Principal have overall responsibility for e-safety within our school. The day-to-day management of this is delegated to the Deputy Principal, the Online Safety Lead.

The Principal/Deputy Principal 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 Online Safety Lead(s) has had appropriate CPD in order to undertake the day-to-day duties.
- All e-safety incidents are dealt with promptly and appropriately.

Online Safety Lead

The designated Online Safety Lead is devolved to The Deputy Principal and Safeguarding Lead, Mrs Helena Bull

The Online Safety Lead will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves 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 Principal.
- Advise the Principal 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 overall responsibility for e-safety incident reporting
- 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 Principal and the Academy Trust, to decide on what reports may be appropriate for viewing.

IT Technical Support Staff (Our Learning Cloud)

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum: Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Software updates are regularly monitored and devices updated as appropriate. Any e-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Online Safety Lead and Principal/Head of School.
- Passwords are applied correctly to all users. Passwords for staff will be a minimum of 8 characters with uppercase and numbers.
- The IT System has a secure password and access policy.

Teaching and Associate Staff

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 E Safety lead/Principal
- Any e-safety incident is reported to the Online Safety Lead or in their absence to the Principal/DSL. If you are unsure, the matter is to be raised with the Online Safety Lead or the Principal/Head of School, to make a decision.
- The reporting procedure is fully understood

All Students

- The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy, which forms part of the induction pack.

- Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the 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 outside of school.

Parents and Carers

Parents play the most important role in the development of their children; 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 parents' evenings, school newsletters and the availability of free online training courses, 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 have to rules in place to ensure that their child can be properly safeguarded. As such all new parents will sign the student Acceptable Use Policy, as part of their induction pack, before their child can be granted any access to school network, ICT equipment or services. The statement set out in Appendix 7 will also be drawn to the attention of parents and carers at appropriate intervals.

Network and Device Management

Purple Oaks Academy uses a range of devices including 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 Impero Software filter, managed by Greenwoods Academies Trust, that prevents unauthorised access to illegal websites, including those sites deemed inappropriate under the Prevent Agenda. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Online Safety Lead and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Principal/Head of School. Web access is logged indefinitely for all users of the ICT systems at Weston Favell Academy.

Email Filtering

Greenwoods Academies Trust uses technology that 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 Academy Trust Network Manager will be responsible for ensuring that passwords are changed as and when required. The use of another person's credentials at any time, is forbidden.

Students who may need support to access their login may be assisted by staff and given simplified login/password until they can be enabled to access their account independently.

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 Principal/Head of School, if there are any concerns.

School Network & the Internet

Use of the school network, with access to the Internet, in school is a privilege, not a right.

Use will be granted to new staff upon signing of the relevant documents on their induction to Purple Oaks Academy.

Access to the network will be granted to new students upon signing and returning their acceptance of the Acceptable Use Policy. These policies apply to all staff and students whether access to the school network or internet is by cable or wireless (or personal mobile account whilst on school premises, including school trips either in the UK or abroad) and on any device, laptop or PC, either school owned or personal.

Email

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, and as such will be given their own email address, based on their network username. 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.

Photos and videos

All parents sign a photo release slip on entry to the school, as part of the Induction Pack they receive; non-return of the permission slip will not be assumed as acceptance.

Social Networking

Purple Oaks Academy is fully supportive of social networking as a tool to engage and

collaborate with learners, and to engage with parents and the wider school community. Any subject specific social media services, permitted for use within Purple Oaks Academy, must have been appropriately risk assessed, managed and moderated in accordance with the Social Media Policies for Staff and Students.

In addition, with reference to images that may be uploaded to such sites, the following is to be strictly adhered to:

- Permission slips (either as hard copy filed in the student record folder or as flagged on the student record on SIMS) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used, if at all.
- All images, videos and other visual resources that are not originated by the school are not allowed unless the owner's permission has been granted.
- Permission to use copyrighted resources must be sought and received before they are used.

Notice and take down policy

Should it come 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.

Reporting E-safety Incidents

Any e-safety incident is to be brought to the immediate attention of the Online Safety Lead, or in their absence the Principal or DSL. The Online Safety Lead will assist in taking the appropriate action to address the issue. All staff should make themselves aware of the procedures and the responsible staff involved in this process.

Training and 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. This includes the regular distribution of e-safety information to staff, students and parents. In addition, Purple Oaks Academy will have an annual programme of online e-safety training for teaching and support staff, to be incorporated within the CPD programme. This online e-safety training provides staff with a certificate which must be renewed by further training on an annual basis. This continuous rolling training programme means that staff will always be up to date with the latest issues on e-safety from new and evolving technologies. The school should ensure that aspects of e-safety for students is firmly embedded into the curriculum. Whenever ICT is used in the school, staff will ensure that students are made aware about the safe use of technology and risks as part of the student's learning. If asked, teachers should be able to demonstrate where and how the awareness of risk is imparted to students in lessons. As well as the

programme of training, the school will establish further training or lessons as necessary in response to any incidents. The Online Safety Lead is responsible for recommending a programme of training and awareness for the school year to the Principal for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Principal for further CPD.