OAKS PARK HIGH SCHOOL

ONLINE SAFETY POLICY

POLICY SCHEDULE AND VERSION CONTROL.

Version	**1.0**
Document Owner	**Leena Davda**
Authors	**Leena Davda** **Jose Bordetas**
Version History	**6th February 2018**

- The implementation of this policy will be monitored by the document owner and the IT department.

- The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

- The school will monitor the impact of the policy using:
  Logs of reported incidents.
  Monitoring logs of internet activity (including sites visited) / filtering
  Internal monitoring data for network activity.
  Surveys / questionnaires of students / pupils, parents / carers and staff.
  Using our e-safety yearly programme schedule.

1. INTRODUCTION. WHAT IS E-SAFETY?

E-safety is a term which means not only the internet safety but other ways in which young people communicate using electronic media, e.g. mobile phones. It means ensuring that children and young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies without risk to themselves or others.

The aim of promoting e-safety is to protect young people from the adverse consequences of access or use of electronic media, including from bullying, inappropriate sexualised behaviour or exploitation

Currently the internet technologies children and young people are using both inside and outside of the classroom or school environment include:

- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Oaks Park High School recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement we at Oaks Park High School want to ensure that the Internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding

To enable this to happen we have taken a whole school approach to E-safety which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's ICT infrastructure and technologies.

Oaks Park High School has developed an E-safety yearly programme to ensure our IT users (governors, staff, students, parents and our community) are fully aware and properly supported when using any ubiquitous Internet connected devices. As a school we are committed to make Internet secure, ensuring that all IT users are educated as to the risks that exists when using the Internet and that themselves can take an active part of promoting a safe Internet environment.

2. THE PURPOSE AND THE SCOPE OF THIS POLICY.

This policy applies to all members of the school (this includes Governing body, staff, students , parents / carers, visitors, volunteers, external contractors and community users) who have access to and are **Users** of the school IT systems.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school .

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Oaks Park High School will ensure that through our whole school yearly E-safety Programme we have the elements in place to enrich, safeguard and empower every IT Internet user in our school.

Here is an example of elements that are included in our E-safety Programme each year:

- E-safety training for staff, students, parents and community.
- Several member of staff with responsibilities on E-safety across the school.
- A range of acceptance policies the are frequently reviewed and updated.
- Information to parents and community that highlights safe practice for children and young people when using the Internet and other digital technologies.
- Supervision of pupils when using the Internet and digital technologies.
- E-safety embed into their normal curriculum that is aimed at ensuring safe use of Internet and digital technologies.
- A robust monitoring, auditing and reporting procedure for abuse and misuse.
- A complete audit of each year E-safety programme is in place as well. This enables us to improve on our practices and make sure that our programme is upto to date and current with the latest technologies/topics and it is engaging for all stakeholders.

3. ROLES AND RESPONSIBILITIES

As E-Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. All members of our school know who our designated E-safety Coordinator is.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

The governing body will review annually this policy as well as the school safeguarding procedures and their implementation.

Headteacher and SLT

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Coordinator.

The Headteacher and (at least) another member of the Senior Leadership Team is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator.

Staff (teaching and support staff)

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP).
- they report any suspected misuse or problem to the Headteacher / Senior Leader ; Online Safety Coordinator
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems.

- online safety issues are embedded in all aspects of the curriculum and other activities.
- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Students

Need to ensure that:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practices when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website / Learning Platform and online student records.
- their children's personal devices in the school (where this is allowed).

4. INFRASTRUCTURE AND CORRECT USE OF TECHNOLOGIES

The school is responsible for ensuring that the school / infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. We will also ensure that the relevant people named in these sections will be effective in carrying out their online safety responsibilities.

School infrastructure will be managed in ways that ensure that the school meets recommended industry standard technical requirements.

As part of our yearly IT maintenance programme, there will be regular reviews and audits of the safety and security of the school IT infrastructure and the services we provide to our users.

All users will be provided with a username and secure password by the IT department. Users are responsible for the security of their username and password and will be required to change their passwords periodically.

Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by LGFL filtering provider and other local filtering services on our Infrastructure. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes Internet filtering should ensure that children are safe from terrorist and extremist material (and many other dangers) when accessing the internet.

School IT department staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software and thread management tools.

Use of Internet facilities and digital technologies

Oaks Park High School will seek to ensure that Internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

The school expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions in this policy and the AUPs: These expectations are also applicable to any voluntary, statutory and community organisations that makes use of the school’s IT facilities and digital technologies.

Users shall not:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - Indecent images of children
    - Promoting discrimination of any kind
    - Promoting racial or religious hatred
    - Illegal acts or promoting illegal acts
    - Any other information which may be offensive to peers or colleagues e.g. abusive images; promotion of violence; gambling; racist; sexist; homophobic or religious hatred material

The School recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites or material may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and also permission is given by senior leaders, so that the action can be justified, if queries are raised later.

The E-safety policy works in conjunction with the User Acceptance Policies, therefore IT users of the school facilities should comply with all of our policies when using the Internet and the school IT infrastructure.

BYOD

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile personal devices in a school context is educational. The mobile technologies policy should be consistent with and interrelated to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage.

Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

The school Acceptable Use Agreements for staff, students and parents/carers will give consideration to the use of mobile technologies.

The school allows:

	School Devices		Personal Devices		
	School owned for single user	School owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*YES*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

Removable Storage Devices (RSD).

Over recent years, staff have increasingly needed to be fully mobile and connected, often taking information home or out of the school in order to maintain productivity and deliver services efficiently and effectively.

Staff need to think whether the use of RSD, e.g. USB stick, is appropriate and secure.
Staff can access student data securely using Google Drive or RDS provided to staff (always use platforms and technologies the school has provided as they are secure).
Data stored on a personal USB stick is, generally, not encrypted and it does not comply with DP or GDPR.
Do not store sensitive information on portable devices that are not fully encrypted and school managed.

Communication & Sharing

Social Media:

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held
responsible, indirectly for acts of their employees in the course of their employment. Staff
members who harass, cyberbully, discriminate on the grounds of sex, race or disability or
who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school
- The school effectively responds to social media comments made by others according to a defined policy or process
- The school's use of social media for professional purposes will be checked regularly by SLT or designated individual to ensure compliance with the school policies.

Please refer to our Social Media policy for more information.

Video/Photos.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Written permission from parents or carers will be obtained before photographs of students / are published on the school website / social media / local press.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school / events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school / into disrepute.

Students / must not take, use, share, publish or distribute images of others without their permission.

Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

Students full names will not be used anywhere on a website or blog, particularly in association with photographs.
Student's / work can only be published with the permission of the student and parents or carers.

5. E-SAFETY OUTSIDE THE SCHOOL NETWORK ENVIRONMENT

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Schools must, through their Online Safety Policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and **outside** school. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

The school might impose disciplinary penalties for inappropriate behaviour which include Incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place **outside** of the school, but are linked to membership of the school.

As a school we make sure that our students and staff have the knowledge, tools, processes and training necessary to deal with any e-safety incidents in a restricted or unrestricted Internet environment. Promoting a safe use of Internet technologies in a ubiquitous way.

6. EDUCATION AND TRAINING.

Students

Our E-safety programme focus in all areas of the curriculum and staff are trained each year to make sure they have the knowledge to tackle any e-safety queries, incidents or situation that can arise.

We provide e-safety online training and awareness through our E-safety yearly programme in several way:

- A planned online safety curriculum should be provided as part of Computing / PSHE / other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Students are taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information. Students / pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students / pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- We ensure that children are safe from terrorist and extremist material on the internet.
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies the internet and mobile devices in lessons where internet use is pre-planned, staff follow best practice in that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Staff

We understand that it is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered through each year as part of our E-safety Yearly Programme:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and other policies.
- It is expected that some staff will identify online safety as a training need within the performance management process,
- The Online Safety Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator will provide advice / guidance / training to individuals as required.

Governors, parents, carers, community,visitors, contractors and community users will also be included in our E-safety Programme with specific training and events for each groups following e-safety standards.

MONITORING, INCIDENTS AND SANCTIONS

Oaks Park High School recognises the need to have regular inspections of policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised. We have robust processes in place to discover, audit and manage our monitoring and reporting of e-safety incidents.

Monitoring

Monitoring the safe use of the Internet and other digital technologies goes beyond the personal use of the Internet and electronic mail a pupil or member of staff may have. Oaks Park High School recognises that in order to develop an effective whole school E-safety approach there is a need to monitor patterns and trends of use inside school and outside school.

With regard to monitoring trends, within the school and individual use by school staff and pupils, Oaks Park High School will audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school are influenced by a range of national and Local Authority guidance documents and will include the monitoring of content and resources.

Another aspect of monitoring, which our school will employ, is the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

Monitoring of IT facilities and internet use by staff and technical staff on a daily basis to make sure students and staff adhere to this and other IT policies.

Classroom management software is in place for facilitate staff to supervise student behaviour as well as improve their teaching and learning using digital technologies.

Several internet filtering services are used to Monitor and Report inappropriate use of the Internet and they are daily monitored by our behaviour management team and technical staff.

Incidents and Sanctions

Oaks Park High School has been careful to develop policies and procedures to support the innocent in the event of a policy breach and enable the School to manage such situations in, and with, confidence.

Where there is inappropriate or illegal use of the Internet and digital technologies, the following sanctions will be applied:

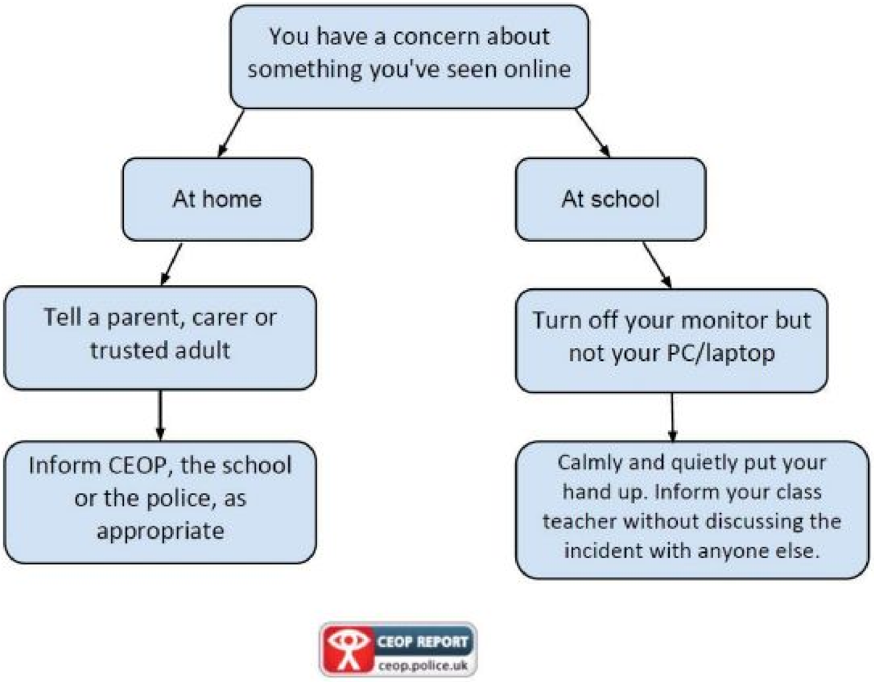
- **Pupils** will be disciplined according to the behaviour policy of the school and may have access to the school's ICT facilities limited or suspended temporarily or permanently.Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

- **Adults** (Staff, Volunteers and other users) Breaches of the policy by staff will be considered under the school's disciplinary policy.Volunteers and other users of the school IT infrastructure/services breaching the policy may have IT access and access to the school removed. Serious breaches which may include unlawful will be reported to the Police and/or other regulatory bodies.

  If inappropriate material or data is accessed, users are required to immediately report this to the IT department.

STUDENT FLOW DIAGRAM FOR CONCERNS

Student Flow Diagram


You have a concern about something you've seen online
At home
At school
Tell a parent, carer or trusted adult
Turn off your monitor but not your PC/laptop
Inform CEOP, the school or the police, as appropriate
Calmly and quietly put your hand up. Inform your class teacher without discussing the incident with anyone else.
CEOP REPORT
ceop.police.uk