E Safety Policy

E Safety Policy

Reviewed March 2026 Review due March 2028

Introduction

West Oaks School e-safety policy aims to create an environment where pupils, staff, parents, governors and the wider school community work together to inform each other of ways to use the internet responsibly, safely and positively.

Through teaching ICT and Computing we equip children and young people to participate in a rapidly changing world where work and leisure activities are increasingly transformed by technology. We enable them to find, explore, analyse, exchange and present information in a varied and stimulating way.
ICT skills are a major factor in enabling them to be confident, creative and independent learners. As the aims of ICT are to equip children and young people with the skills necessary to use technology to become independent learners, the teaching style that we adopt is as active and practical as possible. We provide suitable learning opportunities for all children and young people by matching the challenge of the task to the ability and experience of the child.

Internet technology helps pupils learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The e-safety policy encourages appropriate and safe conduct and behaviour when achieving this.
Pupils, staff and all other users of school related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour. These agreements and their implementation will promote positive behaviour which can transfer directly into each pupil's adult life and prepare them for experiences and expectations in the workplace. The policy is not designed to be a list of prohibited activities, but instead a list of areas to discuss, teach and inform, in order to develop positive behaviour and knowledge leading to a safer Internet usage and year on year improvement and measurable impact on e-safety. It is intended that the positive effects of the policy will be seen online and offline; in school and at home; and ultimately beyond school and into the workplace.

West Oaks School E-safety Policy

The school e-safety policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider school community who use, have access to or maintain school and school related Internet, computer systems and mobile technologies internally and externally.
The school will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding ICT and internet usage both on and off the school site. 'In Loco Parentis' provision under the Children Act 1989 also allows the school to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

The e-safety policy covers the use of:

- School based ICT systems and equipment
- School based intranet and networking

- School related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing.
- School ICT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets
- Pupil and staff personal ICT equipment when used in school and which makes use of school networking, file-serving or Internet facilities.
- Tablets, mobile phones, devices and laptops when used on the school site.

Managing Information Systems

Securely maintaining information

It is important to review the security of the whole system from user to internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and learners

Local Area Network (LAN) security issues include:

- Users must act reasonably - e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For West Oaks staff, flouting electronic use policy is regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date; through regular monthly patching
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with WPA2 PSK (pre-shared key).
-

Wide Area Network (WAN) security issues include:

- West Oaks School broadband firewalls are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership between partner organisations. The Link School broadband network is protected by a cluster of high-performance firewalls at the internet connecting nodes.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used unless it has been encrypted and virus checked.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the network will be regularly checked.
- System capacity in relation to storage will be checked regularly.
- The use of user logins and passwords to access the network will be enforced.

Filter Management.

- The school's broadband access provides filtering appropriate to the age and maturity of learners. There is flexibility in the filtering system to allow for changes in provision depending on the learning required.

Surfprotect works via Standard Browsing Categories and has a default policy set by Exa Networks. West Oaks School has it's own tenancy, allowing or blocking URLs or full categories as required.

- Any breaches in filtering should be reported to the ICT Support and/or emailed to the ICT Development Manager simon.wilson@westoaksschool.co.uk .
- If staff or learners discover unsuitable sites, the URL will be reported to the respective Head of School who will then record the incident and escalate the concern as appropriate.
- The school filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies. The academy's access strategy will be designed by educators to suit the age and curriculum requirements of the learners, with advice from The ICT Development manager.

Monitoring the e-safety policy:

The e-safety policy will be actively monitored and evaluated by an e-safety committee. This committee will comprise:

- E-safety Co-ordinator/Officer (Anna Stevens)
- Principal (Keeley Murray)
- Designated Safeguarding Officer (Anna Stevens)
- Teaching Staff
- Assistant Director of Operations (Simon Wilson)
- Governor(s)

In the event of an e-safety incident, the following people will be informed within school (School E-safety Coordinator, ICT Development Manager.)

E-safety policy review and evaluation schedule:

- The E-safety Policy and Acceptable Use Policy are reviewed at or prior to the start of each academic year. Additionally, the policy will be reviewed promptly upon:
- Serious and/or frequent breaches of the acceptable Internet use policy or other in the light of e-safety incidents.
- New guidance by government/LA/safeguarding authorities.
- Significant changes in technology as used by the school or pupils in the wider community.
- E-safety incidents in the community or local schools which might impact on the school community.

- Advice from the Police and/or the Leeds Safeguarding Partnership.
- The E-Safety policy review will be documented in the school development plan and school self-evaluation and improvement profiling.
- The Management Committee will receive a report on the progress, evaluation, impact and this report will include suitably redacted accounts and statistics of e-safety incidents and how these have been resolved, and counter measures implemented.
- In line with OFSTED recommendations, it is also useful to consult with pupils over the policy and to ask for their opinion on keeping themselves safe when using the Internet.

School Management and e-safety

The School Senior Leadership team is responsible for determining, evaluating and reviewing e-safety policies to encompass teaching and learning, use of school IT equipment and facilities by pupils, staff and visitors, and the agreed criteria for acceptable use by pupils, school staff and governors of internet capable equipment for school related purposes or in situations which will impact on the reputation of the school, and/or on school premises.

- The E-Safety policy is a result of a continuous cycle of evaluation and review based on new initiatives, and partnership discussion with stakeholders and outside organisations; technological and Internet developments, current government guidance and school related e-safety incidents. The policy development cycle develops good practice within the teaching curriculum and wider pastoral curriculum. Regular assessment of strengths and weaknesses help determine inset provision for staff and governors and guidance provided to parents, pupils and local partnerships.
- E -safety provision is always designed to encourage positive behaviours and practical real-world strategies for all members of the school and wider school community.

The school E-safety Co-ordinator:

The school has a designated E-safety Coordinator [Anna Stevens] who reports to the SLT and Governors and coordinates e-safety provision across the school and wider school community.

- The school E-safety Co-ordinator is responsible for e-safety issues on a day to day basis and also liaises with LA contacts, filtering and website providers and the ICT Development Manager.
- The school E-safety Co-ordinator maintains a log of submitted e-safety reports and incidents.
- The school E-safety Co-ordinator audits and assesses inset requirements for staff, support staff and Governor e-safety training, and ensures that all staff are aware of their responsibilities and the school's e-safety procedures. The co-ordinator is also the first port of call for staff requiring advice on e-safety matters.
- Although all staff are responsible for upholding the school e-safety policy and safer internet practice, the E-safety Co-ordinator, the Principal and Vice Principal, Heads of School and the ICT Development Manager are responsible for monitoring internet usage by pupils and staff, and on school machines, such as laptops, used off-site.
- The E-safety Coordinator is responsible for promoting best practice in e-safety within the wider school community, including providing and being a source of information for parents and partner stakeholders.

- The school E-safety coordinator (along with the ICT Development Manager) should be involved in any risk assessment of new technologies, services or software to analyse any potential risks

Governors' responsibility for e-safety:

- At least one Governor is responsible for e-safety (John Hayton), and the school E-safety Co-ordinator will liaise directly with the Governor with regard to reports on e-safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community. The E-safety Co-ordinator will be responsible for auditing Governor e-safety training and inset requirements.

ICT support staff and external contractors:

- External ICT support staff and technicians are responsible for maintaining the school's networking, IT infrastructure and hardware. They are aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the Internet is secure. They further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.
- Support staff maintain and enforce the school's password policy.
- External contractors, such as VLE providers, website designers/hosts/maintenance contractors are made fully aware of and agree to the school's e-safety Policy. Where contractors have access to sensitive school information and material covered by the Data Protection Act, for example on a VLE, school website or email provision, the contractor should also be DBS checked. A Service Level Agreement (SLA) is in place to provide school standard provision and support.

Staff:

- All staff need to ensure that they are aware of the current school e-safety policy, practices and associated procedures for reporting e-safety incidents.
- All staff will be provided with e-safety induction as part of the overall staff induction procedures.
- All staff need to ensure that they have read, understood and signed (thereby indicating an agreement) the Acceptable Use Agreement relevant to Internet and computer use in school. All staff need to follow the school's social media policy, in regard to external offsite use, personal use (mindful of not bringing the school into disrepute), possible contractual obligations, and conduct on Internet school messaging or communication platforms, for example email, VLE messages and forums and the school website.
- All staff need to rigorously monitor pupil Internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the school site.
- Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.
- Be aware of online propaganda and help pupils with critical evaluation of online materials.
- Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with learners or parents/carers is required.
- Mobile phone and devices will be switched off unless issued by the school.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff must not use personal devices such as mobile phones or cameras to take photos or videos of learners and will only use work-provided equipment for this purpose.
- If a member of staff breaches the academy policy then disciplinary action may be taken.

Designated Safeguarding Lead:

- The Designated Safeguarding Officer is trained in specific e-safety issues. Accredited training with reference to child protection issues has been accessed.
- The Designated Safeguarding Officer can differentiate which e-safety incidents are required to be reported to CEOP, local Police, LADO, Local Safeguarding Children's Board, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.
    - Possible scenarios might include:
    - Allegations against members of staff.
    - Computer crime – for example hacking of school systems.
    - Allegations or evidence of 'grooming'.
    - Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication. o Producing and sharing of Youth Produced Sexual Imagery (YPSI)
- Acting 'in loco parentis' and liaising with websites and social media platforms such as Twitter, Instagram, Snapchat and Facebook to remove instances of illegal material or cyber bullying.

Pupils:

- Are required to use school internet and computer systems in agreement with the terms specified in the school Acceptable Use Policies. Pupils are expected to sign the policy to indicate agreement, and/or have their parents/guardians sign on their behalf.
- Pupils need to be aware of how to report e-safety incidents in school, and how to use external reporting facilities, such as the Click CEOP button or Childline number.
- Pupils need to be aware that school Acceptable Use Policies cover all computer, internet and mobile technology usage in school, including the use of personal items such as phones.
- Pupils need to be aware that their Internet use out of school on social networking sites such as Instagram is covered under the Acceptable Use Policy if it impacts on the school and/or its staff and pupils in terms of cyber bullying, reputation, or illegal activities.

The 4 Cs of online safety are a framework that categorizes online risks into four areas:

Content
The type of content a child may be exposed to, such as profanity, violence, or sexual content

Contact
The type of contact a child may have with others online, such as unwanted contact or bullying

Conduct
The type of behaviour a child may engage in online, such as sharing personal information

Commerce
The type of commercial activity a child may be exposed to online, such as embedded marketing

The 4 Cs of online safety are used to help identify, understand, and address online risks. They can be applied to any online activity, such as using a new app, game, or social media channel

Learners Use of Personal Devices

- Mobile phones will be handed in to reception, they will be placed in an individual names wallet and stored securely until they are returned at the end of the school day. Mobile phones will not be taken on outdoor activities.
- Parents/Carers are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Children and young people should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Parents and Guardians:

- It is hoped that parents and guardians will support the school's stance on promoting good internet behaviour and responsible use of IT equipment and mobile technologies both at school and at home.
- The school expects parents and carers to sign the school's Acceptable Use Agreement, indicating agreement regarding their child's use and also their own use with regard to parental access to school systems such as websites, forums, social media, online reporting arrangement, and questionnaires.
- The school will provide opportunities to educate parents with regard to e-safety through the school website and drop in sessions

Other users:

- Other users such as school visitors, or wider school community stakeholders or external contractors should be expected to agree to a visitor's AUA document specific to their level of access and usage.
- External users with significant access to school systems including sensitive information or information held securely under the Data Protection Act should be DBS checked. This includes external

contractors who might maintain the school domain name and web hosting – which would facilitate access to cloud file storage, website documents, and email.

How will the school provide e-safety education?

Curriculum

'Teaching online safety in school (DfE, June 2022) outlines to schools the importance of helping children and young people not only use the internet safely, but also give them opportunities to learn how to behave online. Throughout the new compulsory Relationships (Sex Education) and Health Education pupils will be taught what positive, healthy and respectful online relationships look like.

The PSHE curriculum will following the underpinning knowledge and behaviours:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Online behaviour
- How to identify online risks
- How and when to seek support

Throughout the curriculum teaching about potential harms will include:

- Age restrictions
- Content: How it can be used and shared
- Disinformation, misinformation and hoaxes
- Fake websites and scam emails
- Fraud (online)
- Password phishing
- Personal data
- Persuasive design which keeps 'users online for longer than they might have planned or desired'
- Privacy settings
- Targeting of online content
- Abuse (online)
- Challenges [to do something and post about it]
- Content which incites...hate, violence
- Fake profiles
- Grooming
- Live streaming
- Pornography
- Unsafe communication
- Impact on confidence (including body confidence)
- Impact on quality of life, physical and mental health and relationships
- Online vs. offline behaviours
- Reputational damage

- Suicide, self-harm and eating disorders
- E-safety is accessed as part of pastoral care – form time activities, assemblies, year group presentations, tutorial opportunities.
- E-safety events – such as Safer Internet Day and Anti Bullying Week.

Parents/Carers – information and events:

E-safety information is directly available to parents via the school website which is updated with the latest e-safety news and issues.
School will take advantage of occasions when parents are in school to promote e safety.

Staff – inset and training:

- E-safety information is directly delivered to staff annually during safeguarding training.
- A planned programme of e-safety training opportunities is available for staff, including on site inset, whole staff training, online training opportunities (for example E-safety Support courses), external CPD courses, accredited CPD courses, (for example CEOP) and Coordinator training.
- The E-safety Coordinator should be the first port of call for staff requiring e-safety advice.

Governors - training:

- E-safety information will be directly delivered to governors.
- Governors will be provided access to specific governor training provided externally by the LA through the Governors training programme.

ICT support staff – contractors, filtering and monitoring:

- IT support staff and contractors will ensure that bought in hardware and software solutions feature Built in training provision
- Support staff and contractors will be DBS checked and agree and sign the school's e-safety AUA.
- IT technical support staff and network managers have relevant industry experience and Microsoft/Cisco certified qualifications.

Policy guidance for handling personal data, dealing with freedom of information requests, and complying with privacy regulations pertaining to website data:

All of these areas are regulated by the Information Commissioner (ICO), and every UK organisation has to comply with the responsibilities and obligations as defined by the ICO. Schools are no different to any other organisation in this regard. The ICO guidance on how to comply with these obligations is updated regularly. The Link School refer directly to this guidance in these areas.

When disposing of computer equipment, schools needs to ensure all data, including personal data is wiped, not deleted from storage.

Use of ICT facilities for curriculum teaching and learning:

Use of the Internet and ICT facilities should be clearly planned prior to the activity. Websites and software Apps should be suggested, Students should be trusted to be responsible when researching the Internet, and teaching staff will consider the age and maturity of the students.

General Data Data Protection and e-safety:

The GDPR sets out the **key principles** that all personal data must be processed in line with.

- **Data must be:** processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected

There are also **stronger rights for individuals** regarding their own data.

- **The individual's rights include:** to be informed about how their data is used, to have access to their data, to rectify incorrect information, to have their data erased, to restrict how their data is used, to move their data from one organisation to another, and to object to their data being used at all.

- The General Data Protection Act is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.
- Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies. Personal and sensitive information should only be sent by e mail when on a secure network.
- Personal data should only be stored on secure devices. In other words, only computers, servers, file-servers, cloud space, or devices which require a user name and password to access the information.
- Secure accounts need to be logged off after use to prevent unauthorised access. Personal e-mails should not be used for school business.

Personal information on the school website:

- No material defined as 'personal information' under the General Data Protection Act will be used on the school website.
- The School considers staff privacy issues carefully with regard to publishing staff email addresses, staff lists, photos of staff, staff qualifications and any other personally identifying information.

E-safety and the Law:

This e safety policy takes cognizance of the following legislation;

The Education and Inspections Act 2006 (Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site. Also, staff can confiscate mobile phones if they cause disturbance in class breach the school behaviour policy.)

Computer Misuse Act 1990, sections 1-3 Data Protection Act 1998 Freedom of Information Act 2000 Communications Act 2003 section 1,2 Protection from Harassment Act 1997 Regulation of Investigatory Powers Act 2000 Copyright, Designs and Patents Act 1988 Racial and Religious Hatred Act 2006
General Data Protection Regulations
Protection of Children Act 1978 Sexual Offences Act 2003

Schools have a 'duty of care' to pupils, and as such act "in loco parentis." Under the Children Act 1989, this enables schools to remove personal information, cyber bullying and comments relating to school pupils as if they were the child's parent. Facebook in particular has provision for using 'in loco parentis' when reporting cyber bullying. This is relevant to all schools.

Useful links to external organisations:

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact local Police.

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Monitoring and review

This policy has been approved by the governing body and will be reviewed annually or in the light of new guidance from the Department for Education or Local Authority.

Signed (Principal): ……

Signed (on behalf of the governors): …….