Old Vicarage School

E-Safety Policy

This policy applies to the whole school including the Early Years Foundation Stage (EYFS).

This policy should be read in conjunction with the School's Child Protection & Safeguarding Policy, Anti-Bullying Policy, Acceptable Use of Technology Agreement – Pupils and Parents and, where relevant, the iPad Home-School Agreements (Years 3 – 6).

Old Vicarage School recognises that technology has transformed the lives of children and young people, providing them with enormous opportunities to communicate, learn, research and play.

We seek to ensure that our pupils have a positive experience of technology and appreciate its relevance in our society. We want the use of technology to be presented as a creative and fascinating process in which pupils are encouraged to use their own initiative, imagination, reasoning and investigative skills. We expect all our pupils to become thoughtful users of technology and the internet and develop these capabilities to the best of their ability.

However, technologies present risks as well as benefits. Internet use for home, social and leisure activities is used by all sectors of society. Much of the material on the internet is unsuitable for children and young people who may have unlimited and unrestricted access via mobile phone networks, (ie 3G, 4G &5G) which some children may use to sexually harass their peers, share indecent images consensually and non-consensually and view and share pornography and other harmful content. In addition, there is information on weapons, crime, terrorism, violence, extremism and racism, access to which would be more restricted elsewhere.

This document sets out the policy and practices for the safe and effective use of the internet at Old Vicarage School. It addresses Contact & Content, and Conduct & Commerce as follows:

- Contact & Content
    - Guided educational use
    - Remote learning
    - Safe use of the internet outside school
    - Smart/mobile/ camera devices
- Conduct & Commerce
    - Internet Safety
    - Technical Infrastructure & School website
- Safeguards
    - Monitoring IT Systems
    - Child Protection and Safeguarding

Contact & Content

Guided Educational Use

The purpose of internet use in school is to raise educational standards, promote pupil achievement, support the professional work of staff and enhance the management information and business administration systems. Internet use is a part of the statutory curriculum and the School has a duty to provide pupils with quality Internet access as part of their learning experience. We recognise that online safety requires us to be aware of the risk of pupils being exposed to illegal, inappropriate or harmful content (for example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalism and extremism). There is also the risk of being subjected to harmful online interaction with other users, for example peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal financial or other purposes.

Pupil access to the School internet is designed expressly for pupil use. Our teachers guide pupils in on-line activities that support the learning outcomes planned for the pupils' age and maturity. Aimless surfing is not permitted.

The School has a secure Virtual Learning Environment (VLE) which allows the us to share information and materials with pupils and their parents via the web. The VLE also enables teachers to select and introduce specialist educational applications into the curriculum to stimulate discussion, promote creativity and enhance and extend learning.

Pupils in certain age groups are provided with iPads on a 1:1 basis to support their learning at school and for educational purposes at home. All internet traffic on the iPads is directed through the school's server and use is monitored and protected.

Pupils are educated in the safe and effective use of the Internet and other forms of digital communication.

Remote Learning

If the School is subject to a period of unavoidable and long term closure, the School will provide continuity of education to all pupils through a process of remote (online) learning.

All Remote Learning will be delivered via our secure VLE (Firefly) and video conferencing software (Teams).

Staff will be expected to follow the School's safeguarding guidance when delivering virtual lessons, especially where webcams are involved.

Safe use of the Internet outside school

Sometimes children can be given unsupervised access to the internet, outside school (eg at home). This, potentially, allows them to access all kinds of society and materials. We believe that by fostering a sensible approach at home and at School, we will be able to equip children with the skills they need to become responsible users of technology and help protect them from harm.

The school provides iPads to all pupils and year 5 and 6 will have access to these at home and other year groups in a remote learning scenario. We recommend using these provided devices as content filters/monitoring and app restrictions are on by default, however parents should still monitor what their child is accessing.

We ask parents to consider:

- Discouraging the use of social networking sites under the age of 13.
- Talking to their child about what they are doing on-line and, if possible, restrict their computer use to a shared area at home so they can be aware of sites that are being accessed
- Ensuring their child does not give out any personal details of any kind which may identify them (including telephone numbers and addresses) to people they may meet online, including on games consoles
- Ensuring that appropriate content filters are switched on

- Ensuring that a Parental Control App like qustodio.com or https://www.kaspersky.co.uk/safe-kids is installed on any mobile devices used by sub teen children.
- Encouraging the use of search engines designed specifically for children such as www.safesearchkids.com and www.swiggle.org.uk

Smart/Mobile/Camera devices

Only Year 5 and 6 pupils who make their own way to/from School are permitted to bring a mobile phone into school. All mobile phones are handed into the School Office on arrival and collected at the end of the School day. We strongly recommend that a parental control app is installed on all private mobiles brought into school by pupils.

Visitors may only use their own smart/mobile devices in the reception area and for recording their child's performance in an assembly or school production in the School Hall.

Only School devices (iPads, mobiles, cameras) should be used by staff to take photographs of School activities. If a member of staff must use a personal device (e.g. on a school trip), they should download the photos to the School system as soon as possible and delete them from their personal device.

The use of camera devices of any sort is not permitted in toilet, washroom or changing areas.

Conduct & Commerce

The Internet is available to all through a variety of communication devices. Anyone can send messages, discuss ideas and publish material with little restriction. These features make it both an invaluable resource used by millions of people every day, as well as a potential risk to young and vulnerable people

The School is aware that personal online behaviour increases the likelihood of or causes harm, for example making, sending and receiving explicit messages (for example, consensual and non-consensual sharing of nudes and semi nudes and / or pornography, sharing other explicit images and on line bullying). Further commerce poses a risk – for example online gambling, inappropriate advertising, phishing and or financial scams

Internet Safety

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. 21st century life presents dangers from which children and young people need to be protected. At the same time, they need to learn to recognise and avoid these risks – to become "Internet Wise".

Age appropriate lessons are given in both IT and PSHE about the dangers of the Internet and mobile devices. Pupils are not permitted to access social networking sites at School (users should be 13 years+) but we teach the responsible and safe use of social networking sites as we are aware that some pupils do use them outside School.

Pupils are taught about the dangers of cyber-technology and how they can avoid making themselves vulnerable to a range of risks including identity theft, bullying, abuse, grooming and radicalisation. They are taught that it is a criminal offence to send an electronic communication (words and/or images) to another person with the specific intent to cause distress or anxiety. Pupils are encouraged to report any incidents immediately to their parents or a teacher.

If we discover that a pupil is being subjected to cyberbullying (including peer on peer abuse, sexual harassment or sexual violence) , it will be dealt with through the procedures detailed Safeguarding & Child Protection Policy (& in the School's Anti-Bullying Policy) . If staff become aware of sharing of nudes or semi nudes (so called "sexting" incident), it will be reported to the School's Designated

Safeguarding Lead (DSL) and handled in accordance with our safeguarding procedures. The guidance issued by UKCIS will be followed. Information can be found at https://ineqe.com/2021/01/13/ukcis

Technical Infrastructure & Safeguards

All the School computers and pupil iPads are connected to the School internet, across which a range of services are provided to users of the School network. Network access is password protected and users have clearly defined access rights in accordance with their role. All internet and email use is monitored by the School's IT Support Manager.

The School's external IT consultant works with the Bursar and IT Support Manager, to ensure that the IT infrastructure is not open to misuse or malicious attack and that all protection software is up-to-date. The School systems are reviewed regularly with regards to security and data protection.

The School will do all it reasonably can to limit pupil's exposure to potentially harmful or unsuitable content (e.g. pornographic, terrorist and extremist material) through the use of appropriate filters and monitoring systems which are designed to protect pupils, but not over-block or impose unreasonable restrictions as to what can be taught online.

Access to specific educational software is determined by the teaching staff and implemented and monitored by the School's IT Support Manager. Access levels are regularly reviewed to reflect the curriculum requirements and age of pupils. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is permitted.

School Website

The contact details on the School website are the School address, e-mail and telephone number. Personal contact details for staff will not be published. Images that include pupils are selected carefully and pupils' full names will not be used in association with photographs or content.

Parents may advise the School in writing if they do not permit the School to publish images of their child. The Head has overall editorial responsibility and ensures that content is accurate and appropriate.

Parent, pupil and staff access to the School VLE via the public website is username and password protected and individual user types have clearly defined access rights.

Safeguards

Monitoring IT Systems

All staff are made aware of the School's expectations regarding their use of School IT systems, email, the Internet, iPads, mobile phones and camera devices. Staff development in the safe and responsible use of the Internet is provided as necessary.

Pupils and their parents from Year 2 upwards are required to read and sign the School's Acceptable Use of Technology Agreement. Pupils who have been provided with their own iPad by the School are also required to read and sign a further agreement with regards to their use of these iPads both at School and at home.

Despite the School's best efforts, pupils may occasionally be confronted with inappropriate content. Pupils are taught that, if they experience material that they find distasteful, uncomfortable or threatening, they should close the web page and report the incident immediately to the teacher.

Any attempts to access inappropriate content that are identified by the school monitoring systems will be logged by the IT Support Manager. All incidents of misuse will be investigated, recorded and the School's Safeguarding Committee will be notified. Staff are required to report any inappropriate content that gets through the filtering system to the Head and the IT Support Manager who will ensure it is immediately blocked.

Any concern or complaint about staff misuse must be referred to the Head, unless it is the Head in which case the referral must be made to the Chair of Governors.

Child Protection and Safeguarding

The School's Designated Safeguarding Lead (DSL) has lead responsibility for safeguarding and child protection in the School, including on-line and digital safety.

Any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on School computers will be referred to the Police.

If we discover that a pupil is at risk because of online activity (including but not limited to Cyber Crime, Sexual Harassment or Violence, Peer on Peer Abuse or Child Sexual or Criminal Exploitation), it will be treated as a Safeguarding matter and we will follow the procedures detailed in the Child Protection & Safeguarding Policy.

The School may also seek assistance from the Child Exploitation and Online Protection Unit (CEOP) which works with child protection partners across the UK to identify the main threats to children and coordinates activity against these threats to bring offenders to account. Their website, www.thinkuknow.co.uk, contains internet safety advice for children, parents and teachers.

Parent Concerns

If parents have concerns about any of the subjects raised in this policy, they should contact the Head.

Signed:	**Mandy Fawcett**	**Elizabeth McCartney**	**Daniel Handley**
Role:	**Deputy Head**	**Head of ICT (Academic)**	**IT Support Manager**

Last Review:	June 2022
Next Review:	June 2024