ONLINE SAFETY POLICY (This is to replace the current E-Safety Policy)

This policy covers all pupils including the Early Years Foundation Stage (EYFS) and anyone who works within the school community.

INTRODUCTION AND OVERVIEW

The aim of this policy is to ensure a whole school approach to online safety. It applies to all members of the St David's Community (including staff, governors, students/ pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of St David's.

This Policy should be read in conjunction with:

- Most recent version of Keeping Children Safe in Education
- Meeting digital and technology standards in schools and colleges (2022)
- Acceptable Use Policies (AUPs)

At St David's (hereafter referred to as 'the school') we recognise that pupils will have access to technologies that have both positive and negative potential. The school also recognises the enormous benefits - to pupils and staff - of the internet as a means of academic research, for entertainment and for social interaction, and seeks to promote and encourage its effective use. The school is fully aware that online safety is directly related to safeguarding and takes seriously its responsibility to advise students, parents and staff of the significant dangers digital technologies can present when used inappropriately, whether this misuse be deliberate or unwitting.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate or harmful material, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalization, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

Contact: 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.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm, for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying;

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The safe use of ICT is an issue of behaviour, education, infrastructure and monitoring; it is fundamental to safeguarding pupils and staff both in and out of School.

The school takes all reasonable precautions to ensure that users access only age-appropriate material, that content accessed via school devices and systems is appropriately filtered and monitored, and to educate pupils about online dangers. However, experience shows that it is not possible to guard against every danger and so we take a proactive approach to minimising risks whilst also educating pupils so that they can respond appropriately to an unsafe situation. Risks are considerably greater where devices are beyond the school's control. (F6 phones and medical devices) and so the education aspect of online safety is particularly important.

Getting pupils into safe habits when accessing the online world via our systems should enable them to make the right choices when using their own connections. A key part of the online safety support is to share this information with parents.

It is important to be aware that safeguarding concerns can happen solely offline or solely online, but that it is often the case that issues can happen concurrently both in the real world and online. Whenever considering any offline issue the staff involved should always explore whether there is also any online component.

AIMS

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, visitors, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

DEFINITION AND SCOPE

Online safety encompasses use of the Internet and all electronic communications via computers, mobile phones, smart watches, tablets, handheld devices, games consoles and wireless technology both on and off the school site if associated with school or if usage impacts on the school community. It includes, but is not restricted to the following:

Safe online behaviour

- Behaving with respect for others and protecting one's own online reputation
- Having an understanding of what constitutes cyberbullying, nudes and semi-nudes, grooming, abuse, radicalisation, misinformation, disinformation (including fake news) and conspiracy theories.
- Understand the risks associated with the use of AI tools, including that they can produce content that is inaccurate, biased, or inappropriate for young users, the dangers of sharing of personal information including photos, and the possibility of emotional attachment or overreliance on chatbots.

Using online sites safely and responsibly

- Ensuring any posts and comments made online are appropriate and do not bring individuals or the name of the school into disrepute; abiding by any age restrictions for holding an account

Responsible electronic communications

- Via text message, email, group chats and other social networking apps, social media posts and blogs etc.

Protection of personal details

- Ensuring that name, age, address, bank details and other personal details etc. are never shared online or with AI systems.

Exercising judgement when using the Internet

- Accessing only appropriate content on the Internet
- Knowing how to report anything inappropriate and/or suspicious both inside and outside of school
- Checking the validity and reliability of information found online and that produced by AI tools.

Email safety

- Awareness of how to deal with 'spam' and 'phishing' emails, only trusting 'known' senders, particularly when opening attachments.

Security awareness

- Creating strong passwords, keeping passwords private, being aware of viruses and hacking
- Respecting copyright and intellectual property laws when sharing or downloading files
- Knowing how to report an issue both within and outside school
- Talking to a responsible adult about any issues including using CEOP's 'Make a Report' if needed.

OVERSIGHT OF ONLINE SAFETY

Online Safety Committee

The DSL meets with the 'online safety committee' at least once each term to review school processes and discuss any incidents or patterns. This committee consists of The DSL, DDSLs and the IT Co-Ordinator. The IT Manager and the DSL are responsible for evaluating our filtering and monitoring provision and for procuring systems required to support this area.

The online safety committee and its members take responsibility for monitoring the overall effectiveness of our systems and procedures, identifying any education needs that arise and implementing changes in these systems and procedures as necessary.

Reporting Concerns (including Safeguarding concerns)

Online safety is a whole school responsibility and pupils, parents and staff should report any issues or concerns in relation to online activity or digital technology to any member of the Online Safety Committee.

If the matter relates to safeguarding, it should be reported to the Designated Safeguarding Lead or one of the Deputy Designated Safeguarding Leads. If none are available, the matter should be reported to a member of the school's Senior Leadership Team.

If a member of staff believes a child is suffering or likely to suffer from harm, or is in immediate danger, they must contact children's social care and/or the police immediately. Anyone can make a referral of this sort, but the DSLs (or deputies) can support with this and will usually take responsibility for taking this action. Information about how to make a referral can be found in the Safeguarding and Child Protection Policy.

A particular risk faced by young people online is that they may be radicalised or drawn into extremism. All members of staff receive safeguarding training on the Prevent Duty as part of their routine updates, at least annually, in order that they are able to recognise warning signs in relation to a pupil's online or offline behaviour in relation to this risk.

Filtering and Monitoring

As per the most recent KCSIE, the appropriateness of filtering and monitoring systems is a matter for the school and is informed in part by the Prevent Duty. At St David's, online activity is proactively filtered and monitored using commercial products. These products block staff and pupil access to inappropriate sites (e.g. gambling and pornography) and provide reports of any attempts by pupils and/or staff to access inappropriate sites. The list of sites blocked by these filters are routinely updated by the service providers.

As per the Department for Education filtering and monitoring standards, the school:

- Identifies and assigns roles and responsibilities to manage filtering and monitoring systems
- Reviews filtering and monitoring provision at least annually
- Blocks harmful and inappropriate content without unreasonably impacting teaching and learning
- Has effective monitoring strategies in place to meet safeguarding needs

The governing body will review these standards and discuss with the DSL and with IT staff what more needs to be done to support the school to meet this standard.

The school's filtering and monitoring system works on all school-issued devices whether they are on site or away from school. Personal devices are not subject to Filtering and Monitoring, unless accessing school Wi-Fi onsite devices during the school day, which ensures that they cannot access unfiltered content.

To manage the risks presented by the use of AI tools, the schools filtering and monitoring system diverts pupils using school devices into securly's safe AI chat.

Breaches are reported using a categorisation system which is automated but also monitored and managed by the IT Manager. Breaches are then investigated as required by the appropriate member of staff; the decision on who does this will be taken by the DSL of the school.

Pupils and parents should be aware that most social media sites have regulatory age limits. Most sites require members to be over the age of 13. Terms and conditions should be read carefully prior to signing up for an account. The school wired network blocks all social media access during the school day for pupil access (exemptions are via department and permission from a member of SLT).

Google Classroom (GC)

The school's Google Classroom area is an important aspect of our approach to online safety:

- Pupils and parents have access to Online Safety Advice via the Wellbeing Classroom
- Pupils can report concerns to school via the 'Private message' option

GC is a secure area, only available to the St David's community.

- Only members of the current pupil, parent/carers and staff community will have access to GC.
- When staff, pupils etc. leave the school, their account or rights to specific school areas will be disabled**.**

ONLINE SAFETY EDUCATION

Pupils

The school is committed to ensuring pupils are using the Internet and electronic communications in a safe and responsible way. The school expects and promotes good conduct, behaviour and etiquette online both inside and outside of school.

Online safety education is delivered across the school curricula through:

- Lessons in online safety via the Computing and PSHE curricula, including visiting speakers
- Form/House sessions
- School assemblies, house assemblies and Form assemblies
- Parent awareness workshops
- School communications; for example, the School Newsletter and email correspondence
- Staff induction sessions, INSET and training.

Our approach to education of pupils in online safety:

- Encourages pupils tell us when they have concerns.
- Takes pupils through the Acceptable Use of ICT Policy every year in a Computing lesson asking pupils to sign the agreement.
- Educates pupils via the PSHE curriculum about how to stay safe online and how to report concerns, as well as through the assembly programme if/when additional updates are needed.
- Keeps parents informed through workshops and newsletters.
- Reminds pupils regularly (though PSHE curriculum and other opportunities such as House / Form or Whole School assemblies) about the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to anyone.

Staff

It is essential that staff granted access to the school's IT networks receive education and training. This is achieved through the following means:

- Staff induction for new joiners
- Ongoing annual updates plus additional information provided as and when appropriate (for example, when legislation changes or there is a new platform or device to use, or when there is an Online Safety update that needs to be shared sooner)
- Confirmation that staff have read and understand the relevant policies, including:
  - Staff acceptable use policy
  - Staff Code of Conduct
  - KCSIE updates
  - Online Safety Policy
  - Safeguarding and Child Protection Policy
- The school subscribes to a commercial provider of ongoing training overseen by the network manager, currently consisting of Educare or other courses sent to all staff.

Parents

Parents play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours and interactions with digital technologies. The school will provide information about online safety to parents through newsletters and parent information evenings. Parents sign the Acceptable Use agreement on entry at St David's.

Governors

Oversight of the School's Online Safety provision is via the work of the Education and Welfare Subcommittee.
The Online Safety governor is the Chair of the Education and Welfare Sub-Committee, and he meets with the DSL termly to discuss safeguarding matters including online safety.

DEALING WITH ONLINE SAFETY RELATED INCIDENTS

Pupils

The school takes a **zero-tolerance approach** to any cyber bullying issues.

Safeguarding concerns related to online behaviour of pupils must be reported immediately to the DSL or DDSL if they relate to pupil behaviour and to the Headteacher if they relate to staff behaviour. These concerns will be managed in line with the school's Behaviour Policy (pupils) and Staff Code of Conduct (staff).

See **Appendix** for **guidance on what to do in the event of discovering content containing indecent images of children or criminally obscene adult content**

The school will not tolerate behaviours such as:

- Any form of bullying or cyberbullying
- Sharing of nudes or semi-nudes, including those produced with the aid of Generative AI tools.
- Sending or accessing inappropriate online content, including extremist content.
- Posting inappropriate comments/photos on group chats, social media platforms, blogs etc. even when this content is encrypted or in a closed group.
- Taking, uploading or sharing photos, videos or audio recordings without permission
- Unauthorised use of devices, as referred to in the Positive Behaviour Policy.
- Any activity which may bring the school's name into disrepute
- Infringement and disregard for Copyright Law and or intellectual property rights
- Identity theft, including sharing passwords and unauthorised access to school and personal accounts held online.

These will be dealt with according to the Positive Behaviour Policy, the Anti-bullying Policy and the Child Protection and Safeguarding Policy as appropriate.

Staff

- Any breach of the staff acceptable use policy or staff code of conduct should be reported to the Headteacher
- The IT support team may be required to provide technical input as part of the investigation.
- The member of staff involved will be kept informed by the school in line with the Staff Disciplinary Procedure.
- Any disciplinary action will be taken in line with the Staff Disciplinary Procedure.

Searches

If an authorised member of staff has reasonable grounds for suspecting that a pupil / staff member is in possession of data or images that are inappropriate or against the terms of use, s/he is entitled to conduct a search.

Those authorised to conduct a search are listed below:

- The Headteacher
- The Deputy Head
- The Senior Leadership Team
- Online Safety Committee members
- IT Manager

The person conducting the search may search any devices or accounts that the pupil / staff member appears to have control over. Desks and bags can also be searched.

The authorised member of staff should take care that, where possible, searches do not take place in public places such as an occupied classroom or a corridor, in order to protect the privacy of the individual being searched; there must be a witness (also a staff member) and, if possible, they too should be the same gender as the pupil / staff member being searched.

In some cases, if s/he has reasonable belief that there is a risk that serious harm will be caused to a person if the search is not conducted immediately, s/he may conduct this search in the absence of a witness, but only where it is reasonably believed that there is a risk that the serious harm will be caused to a person if the search is not conducted immediately, and where it is not reasonably practicable to summon another member of staff. Care should be taken not to delete material that might be required in a potential criminal investigation.

See **Appendix** for **guidance on what to do in the event of discovering content containing indecent images of children or criminally obscene adult content**

For safeguarding, security, compliance and maintenance purposes, the school reserves the right to examine and/or delete any files that may be held on its systems. Authorised users will monitor and audit equipment, systems, and network traffic. Devices that interfere with other devices or users on the School network may be disconnected. Information Security prohibits actively blocking authorised audit scans. The School's Firewalls and other blocking technologies permit access to the scan sources.

SPECIFIC AREAS OF RESPONSIBILITY

Governing Body: The Chair of Governors will ensure that the School has an Online Safety policy and this is known to all members of teaching staff.

The Headteacher has an obligation to draw up strategies and procedures which aim to prevent Online Safety incidents occurring amongst pupils and pupils**.**

- Discuss development of strategies and review current procedures with the School Leadership Team
- Ensure appropriate training is available to staff
- Ensure that the policies and procedures are brought to the attention of all staff
- Ensure that pupils are aware of the rules and expectations about online behaviour, including how to report concerns (e.g. cyberbullying)
- Ensure that parents/guardians have access to relevant policies via the website and on request.

Designated Safeguarding Lead (DSL) has the lead responsibility for online safety and understanding the filtering and monitoring systems and processes in place. They should be trained in Online Safety issues and be aware of the potential for serious child protection/ safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Radicalisation and exposure to extremist material

The DSL and DDSLs at St David's School are responsible for:

- Making an annual report to the Education and Welfare Subcommittee as part of the safeguarding review.
- Planning and arranging / delivering staff training on online safety.
- Triaging alerts from the Filtering and Monitoring service, and delegating their management to pastoral or safeguarding staff (including managing cases themselves)
- Day-to-day management of the policy and procedures, in liaison with the Head of IT and members of SLT.
- Overseeing support for pupils affected by online safety incidents, usually by delegating support to Form Teacher.
- Determining how best to involve parents/guardians in the solution of individual problems
- Referring cases where there is harm / a risk of harm to the pupil into Children's Services
- Reporting cases where a crime may have been committed against a child to the police

Online Safety Committee: In conjunction with the IT Manager, the Online Safety committee will:

- Meet termly to discuss and review current Filtering and Monitoring provision and other online safety

matters.
- Meet in response to any serious online safety incident to review policy and procedures in the light of the incident.
- Consider and shape the school's response to new technical developments that impact pupil safety, such as the use by pupils and staff of AI tools
- Complete an annual audit of Filtering and Monitoring provision using an external auditing tool (Safe 360/DfE)
- Discuss and review staff training needs

All Staff will:

- Know and implement the current policies and procedures
- Report any concern about or incident of Online Safety whether on-site or during an off-site activity.

Use IT services and devices safely and professionally, in line with the staff Code of Conduct, the staff Acceptable Use Policy and the Use of Artificial Intelligence Policy.

In line with Filtering and Monitoring requirements, ensure that pupils are using devices safely in lessons and other school activities by supervising their behaviour.

Pupils, staff and families, when on site will:

- Use the Internet in support of academic work or personal interests which are consistent with the values of St David's School and the relevant Acceptable Use Policy, the Staff Code of Conduct and the pupil Positive Behaviour Policy.
- Ensure any music, films and files are downloaded legally (i.e. not through unauthorised file-sharing sites), and do not breach copyright laws.
- Use the school's 'safe' internet connection and will not attempt to bypass this service with the use of VPNs or other methods.

LINKS TO OTHER POLICIES

This policy links with:

- Anti-Bullying Policy
- Positive Behaviour Policy
- Child Protection and Safeguarding Policy
- Staff Disciplinary Procedure
- Whistleblowing policy
- Computing and ICT Acceptable Use Policy (Staff)
- Computing and ICT Acceptable Use Policy (Pupils)
- Use of Artificial Intelligence Policy
- Prevent Policy
- Privacy policy

WEBSITES

https://www.ceop.police.uk/safety-centre
www.thinkuknow.co.uk
www.saferinternet.org.uk
www.childnet.com/
https://www.gov.uk/government/publications/channel-guidance
https://www.iwf.org.uk/useful-links/

Policy Reviewed by IT Co-Ordinator	Craig MacGregor/Mark Hayden	February 2026
Reviewed and approved by	SLT	March 2026
Reviewed and approved by	St David's Policy Sub Committee	March 2026
To be reviewed and approved by	EWC	May 2026
To be reviewed and approved by	Board	June 2026
Next Review		January 2027

APPENDIX

Discovery of content containing indecent images of children or criminally obscene adult content

The production and distribution of content that contains indecent images of children is an offence under the Protection of Children Act 1978 and the Sexual Offences Act 2003.

Being in possession of such content carries a penalty of up to five years in prison.

Making content, which includes downloading, storing and printing indecent images of children is an offence that carries a penalty of up to 10 years in prison.

If a user discovers content that contains indecent images of children, it is vital therefore that nothing is done that may lead to prosecution.

In the event of indecent images of children being discovered on a computer the following procedure should be followed:

1. **Lock the computer screen by pressing CTRL+ALT+DEL.**
2. **Do not print, copy, or email the content.**
3. **Do not look at any other content on the computer**
4. **If the images are on a PC, isolate the room where the PC is located. Lock a classroom if appropriate.**
5. **If the images are on a mobile device (eg laptop or ipad) lock the device and take it immediately to the Headteacher or Deputy Head if onsite or as soon as practical if offsite (see further details below).**
6. **Inform the Headteacher and/or the Deputy Head immediately.**

This applies to images produced from real world situations as well as those generated by AI tools.

There is a conditional defence, agreed by the Crown Prosecution Service and the Association of Chief Police Officers, that allows designated IT professionals to access content containing indecent images of children for the purposes of forwarding them on to the Police and the Internet Watch Foundation (the approved body that deals with criminal content online, specifically child sex abuse images and criminally obscene adult content). The Headteacher will nominate designated individuals if this support is needed.

If indecent images of children are found, in consultation with the Headteacher, the Police, and the IWF, one of the designated individuals will access the content and retrieve evidence for the purpose of analysis and possible legal action. Nobody other than those named individuals above should ever attempt to access or distribute material of this nature.

If a user discovers content and there is uncertainty about whether it may be illegal or not, it is better to assume that it is and to follow the procedure above. The legal framework emphasises the importance of reporting illegal content in a timely manner. It is better to assume the worst and to allow a full review to occur swiftly, than leave content unexamined.

Where staff have concerns that school or private email accounts have been compromised and illegal content has been sent, or a link to such content provided, please inform the Headteacher or the Deputy Head immediately. They will authorise a process involving the designated IT professionals to investigate any concern and where necessary, report it to the Police and the IWF.

Content of an illegal nature that is accessed, stored, made, or distributed outside of school using school equipment is subject to the same legal conditions outlined above. Should users detect illegal content on mobile / portable devices provided by the school the equipment should be locked and handed in to the IT Manager as soon as possible. Ideally, this should be within 12 hours of content being discovered. The Headteacher and/or the Deputy Head should be telephoned and emailed immediately. Users should detail the nature of the content but not forward any content itself.

Where users discover content on the School Network that contains what may be deemed to be criminally obscene adult material the procedure above should be followed.

Where staff accounts are found to have accessed or stored pornography via the School Network that does not contain indecent images of children, this will be interpreted as a breach of the ICT Acceptable Use Policy and the Staff Code of Conduct. Disciplinary procedures and dismissal may ensue.