



ONLINE SAFETY POLICY

Jeanetta Liburd	Pr. Eglan Brooks
Headteacher	Chair of Governors

Approved/issue	September 2025	Locations	Appendix to School Handbook Website Headteacher's PA
Review Cycle	2 years		
Next review due	September 2027	Circulation details	Governors Parents via website

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

Key people / dates

 1919 Stanborough Secondary School	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Mrs J. Liburd
	Deputy Designated Safeguarding Leads / DSL Team Members	Mrs E. Hussey; Mrs A. Anderson
	Link governor for safeguarding	Mr R. Murphy
	Curriculum leads with relevance to online safeguarding and their role [e.g., CFL/RSHE/RSE/Computing leads]	Mrs A. Anderson
	Network manager / other technical support	Mr D. Hopa
	Date this policy was reviewed	September 2025
	Date of next review	September 2027

Contents

Key people / dates.....	2
Introduction. What is this policy?	3
Who is it for; when is it reviewed?.....	4
Who is in charge of online safety?	4
How will this policy be communicated?.....	5
Overview	6
Aims.....	6
Further Help and Support	7
Scope	7
Roles and responsibilities	7
Education and curriculum	7
Handling safeguarding concerns and incidents	8
Actions where there are concerns about a child	9
Sexting – sharing nudes and semi-nudes	11
Upskirting	12
Bullying.....	12
Child-on-child sexual violence and sexual harassment.....	12

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

Social media incidents.....	13
Appropriate filtering and monitoring	13
Messaging/commenting systems (incl. email, learning platforms & more)	16
Authorised systems	16
Behaviour / usage principles	16
Online storage or learning platforms	17
School website	17
Social media	18
Staff, pupils' and parents' Social Media presence.....	19
Device usage	20
Personal devices including wearable technology and bring your own device (BYOD)	20
Use of school devices	22
Trips / events away from school.....	22
Searching and confiscation.....	22
Appendix – Roles.....	23
All staff.....	23
Headteacher	24
Designated Safeguarding Lead / Online Safety Lead	25
Governing Body, led by Online Safety / Safeguarding Link Governor –	26
CFL / RSHE Lead/s –	26
Computing Lead – [NAME - don't edit on contents page but in titles themselves]	27
Subject / aspect leaders	27
Network Manager/other technical support roles	28
Data Protection Officer (DPO) – Lorraine McDonald	29
Volunteers and contractors (including tutor)	29
Pupils	30
Parents/carers	30
External groups including parent associations –	30

Introduction. What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into your school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy is subject to biennial review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we will seek to involve staff, governors, pupils and parents in writing and reviewing the policy and make sure the policy makes sense and it is possible to follow it in all respects. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Acceptable Use Policies ensure these are reviewed alongside this overarching policy.

Who is in charge of online safety?

KCSIE makes clear that "the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety)." The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for RSHE will plan the curriculum for their area, it is important that this ties into a whole-school approach.

Background and Online safety risks

In today's secondary schools, the integration of personal devices such as mobile phones and iPads has become increasingly prevalent, reshaping traditional educational practices. These devices serve as versatile tools, offering students access to a vast array of educational resources, interactive learning applications, and communication platforms.

iPads, with their larger screens and diverse range of educational apps, provide an immersive learning experience, allowing students to explore concepts through multimedia presentations, interactive simulations, and digital textbooks.

However, the use of personal devices also raises concerns regarding distractions, cyberbullying, and unequal access to technology. Thus we seek to strike a balance, implementing policies and guidelines that harness the educational potential of these devices while mitigating their potential drawbacks.

At Stanborough School we monitor internet traffic from students own devices while they are onsite using 'Smoothwall'. This also extends to offsite if they are using the Google Chrome browser and are logged on to the browser with school credentials. While onsite, guest devices are connected to a separate network totally isolated from the school's core network.

Self-generative artificial intelligence (AI) has been a significant change, with students having often unfettered access to tools that generate text and images at home or in school. These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for information, but also in terms of plagiarism for teachers and above all safety: none of the mainstream tools have end-user safety settings, most have an age limit of 13 or even 18 and in spite of basic rude words not delivering results, will easily produce inappropriate material. Schools not only need to tackle this in terms of what comes into school but also educating young people and their parents on use of these tools in the home.

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

The continued cost-of-living crisis has meant that children have spent more time online and therefore exposed to all manner of online harms.

Against this background, the Ofcom 'Children and parents: media use and attitudes report 2023' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further. As a school we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore remember to remind about best practice while remembering the reality for most of our students is quite different.

This is striking when you consider that over 95 percent of students have their own mobile phone by the end of Year 7, and the vast majority do not have safety controls or limitations to prevent harm of access to inappropriate material. This is particularly pertinent given that 130,556 cases of self-generated child sexual abuse material were found of 11–13-year-olds (Internet Watch Foundation Annual Report). These were predominantly (but importantly not only) girls; it is important also to recognise more and more older teenage boys being financially extorted after sharing intimate pictures online.

In the past year, more and more children and young people used apps such as snapchat as their source of news and information, with little attention paid to the veracity of influencers sharing news. The 2023 Revealing-Reality: Anti-social-Media Report highlights that this content is interspersed with highly regular exposure to disturbing, graphic and illegal content such as fights, attacks, sexual acts and weapons. At the same time, the Children's Commissioner revealed the ever-younger children are regularly consuming pornography and living out inappropriate behaviour and relationships due to 'learning from' pornography. This has coincided with the rise of misogynistic influencers such as Andrew Tate, which had a significant influence on many young boys over the past year which schools have had to counter.

From the many schools that LGfL spoke to over the past year, there was a marked increase in the number of schools having issues with fights being filmed and shared, a disturbing increase in the cases of self-harm and sexual abuse being coerced with threats of violence (many even in primary schools).

There has been a significant increase in the number of fake profiles causing issues in schools, both for schools – where the school logo and/or name have been used to share inappropriate content about students and also spread defamatory allegations about staff, and also for students, including where these are used to bully others (sometimes even pretending to be one student to bully a second student).

How will this policy be communicated?

This policy will be communicated in the following ways:

- Posted on the school website
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly Reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers, which will be issued to whole school community, on entry to the school, and whenever changed.

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

Overview

Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Stanborough Secondary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world: for the protection and benefit of the children and young people in their care, and for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

The document Keeping Children Safe in Education (KCSIE 2025) identifies four key areas that should be considered in connection with online safety:

- **Content risks:** The child engages with or is exposed to potentially harmful content. This can be violent, gory content, hateful or extremist content, as well as pornographic or sexualised content that may be illegal or harmful, including by being age inappropriate. Content online may be mass-produced or user-generated (including by the child), and it may be shared widely or not.
- **Contact risks:** The child experiences or is targeted by contact in a potentially harmful adult-initiated interaction, and the adult may be known to the child or not. This can be related to harassment (including sexual), stalking, hateful behaviour, sexual grooming, sextortion or the generation of sharing of child sexual abuse material.
- **Conduct risks:** The child witnesses, participates in or is a victim of potentially harmful conduct such as bullying, hateful peer activity, trolling, sexual messages, pressures or harassment, or is exposed to potentially harmful user communities (e.g. self-harm or eating disorders). Typically conduct risks arise from interactions among peers, although not necessarily of equal status.

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

- **Contract/Commerce risks:** The child is party to and/or exploited by potentially harmful contract or commercial interests (gambling, exploitative or age-inappropriate marketing, etc.). This can be mediated by the automated (algorithmic) processing of data. This includes risks linked to ill-designed or insecure digital services that leave the child open to identity theft, fraud or scams. It also includes contracts made between other parties involving a child (trafficking, streaming child sexual abuse).

Further Help and Support

All concerns should be reported in line with the School's Child Protection & Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with have advisors to offer general support.

Beyond this, reporting.lgfl.net has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people. Training is also available via safetraining.lgfl.net

Scope

This policy applies to all members of the Stanborough Secondary School community (including teaching, supply and support staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Depending on their role, all members of the school community should **read the relevant section in Annex A of this document** that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the annex.

It is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues

Education and curriculum

It is important that our school has a carefully sequenced curriculum for online safety that builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, we teach online safety and harms through a whole school approach. This provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils

The following subjects have on-line safety links (see the relevant role descriptors above for more information):

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or CFL – Curriculum for Life)
- Computing

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place). “Parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online” (KCSIE 2025).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

Curriculum reviews consider the key areas of self –image and identity, online relationships, online reputation, online bullying, managing online information, health and wellbeing, privacy and security and copyright and ownership

This is done within the context of an annual online safety audit, which is a collaborative effort led by the DSL and SLT. As a result, an appropriate action plan is put in place.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, CFL/RSHE and Citizenship).

General concerns are handled in the same way as any other safeguarding concern; Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors,

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online safety will be mostly detailed in the following policies

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Policy
- Data Protection procedures and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school takes all reasonable precautions to ensure safeguarding pupils online but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively using the established procedures.

Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

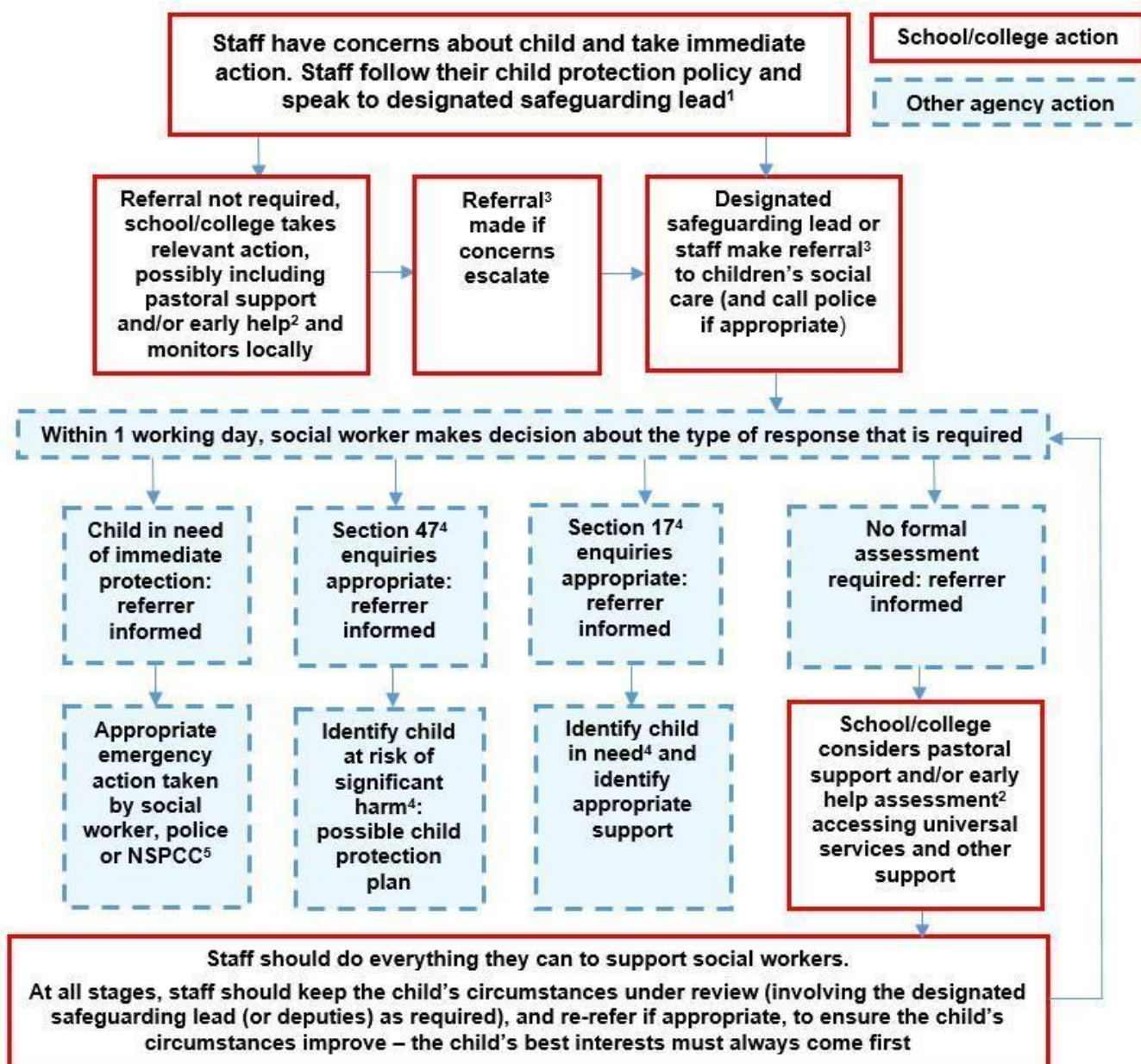
Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Head teacher, in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

The school should evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

Actions where there are concerns about a child

The following flow chart is taken from page 22 of Keeping Children Safe in Education 2023 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



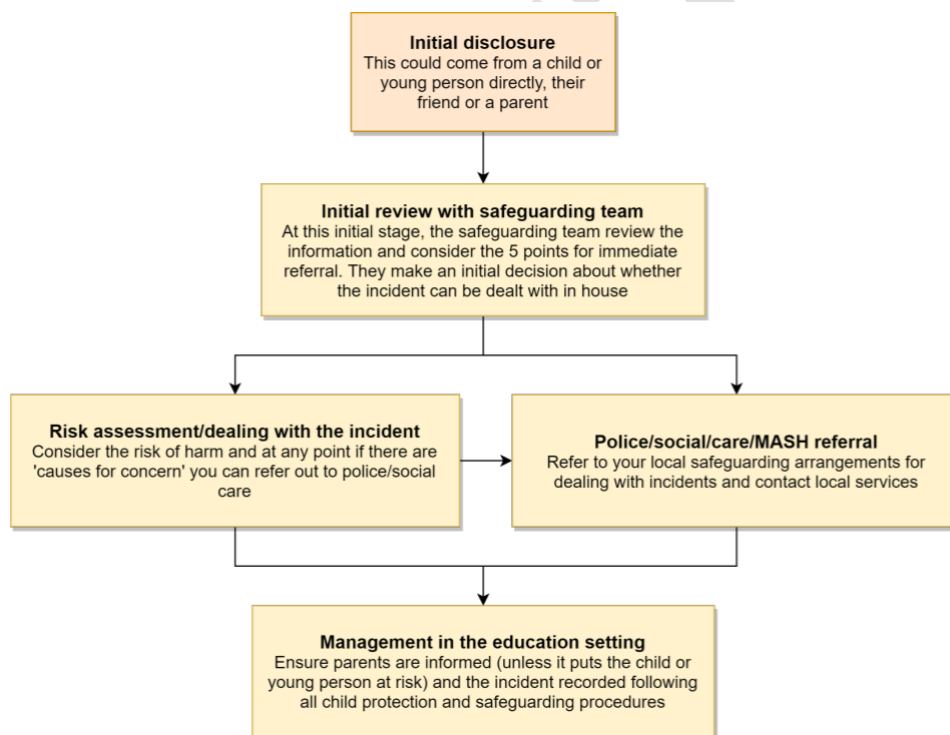
Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

Sexting – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as [Sharing nudes and semi-nudes: advice for education settings](#) to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called [Sharing nudes and semi-nudes: how to respond to an incident](#) for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, [Sharing nudes and semi-nudes – advice for educational settings](#) to decide next steps and whether other agencies need to be involved.



***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter. **Anti-Bullying and Behaviour Management** Policies can be found on the school website: <https://www.spsch.org/policies>

It is important to be aware that in the past 12 months there has been an increase in anecdotal reports of fights being filmed and fake profiles being used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

(Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net)

Child-on-child sexual violence and sexual harassment

Part 5 of Keeping Children Safe in Education covers 'Child-on-child sexual violence and sexual harassment' Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour. Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy on our website: <https://www.spsch.org/policies> under ICT section as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of absence/closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Stanborough Secondary School community. These are also governed by school Acceptable Use Policies and the school social media policy.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Stanborough Secondary School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cybersecurity policies which can be found here: <https://www.spsch.org/policies>. It is important to remember that there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cybersecurity for the first time in 2023.

Data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools, 2023*, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2025, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

Keeping Children Safe in Education has long asked schools to ensure "appropriate" web filtering and monitoring systems which keep children safe online but do not "over block".

Since KCSIE 2025, in recognition of the importance of these systems to keeping children safe, the designated safeguarding lead now has lead responsibility for filtering and monitoring.

The following systems are in place.

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

Technical infrastructure

- Servers, wireless systems and cabling are securely located and physical access restricted;
- All users will have clearly defined access rights to School ICT systems. Details of access rights available to groups of users will be recorded by the IT Manager and will be reviewed annually with a member of the School Leadership Team;
- All users will be provided with a username and secure password by the Network Manager who will keep an up-to-date record of users and their usernames.
- The “administrator” passwords for the school system, used by the IT Manager (or other person) are also available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe);
- Users are responsible for the security of their username and password; they must not allow other users to access the system using their log on details and must immediately report any suspicion or evidence that there is a breach of security;
- The school provides enhanced user-level filtering through the use of “Smoothwall”. In the event that the IT Manager (or other person) needs to switch off the filtering for any reason, or for any user, it must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader);
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager. If the request is agreed, this action will be recorded;
- School IT Support Staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy;
- Remote management tools are used by staff to control workstations and view user’s activity;
- An appropriate system is in place for users to report any actual/potential e-safety incident to the IT Manager/ headteacher /DSL
- 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;
- An agreed procedure is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school system;
- The school does not permit specific files to be downloaded on school workstations. These files include applications, music files and executable extensions.
- Downloading of copyrighted materials without acquiring appropriate rights for them is not allowed; Only IT Support staff are allowed to install programmes on School workstations/portable devices;
- The use of removable media (e.g. memory sticks/CDs/DVDs) by users on School workstations/portable devices is allowed, however they should be scanned for viruses before they are used on the school network;
- The school infrastructure and individual workstations are protected by Sophos Endpoint Protection as well as Coro Cybersecurity platform.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Stanborough School complies with the current filtering and monitoring standards, which require them to:

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

Our Web **filtering** is provided by Smooth wall on school site and for school devices used in the home Changes can be made by **IT Manager: Mr D. Hopa**.

Overall responsibility is held by the **DSL (Mrs Jeanetta Liburd)**.

Technical support and advice, setup and configuration are from the IT Manager

Regular checks are made at least half termly by the IT manager to ensure filtering is still active and functioning everywhere.

An annual review is carried out

According to the DfE standards, “a variety of **monitoring** strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

At Stanborough Secondary School we use LanSchool to monitor pupil accessible computers usually located in places like computer labs, library. Smoothwall logs and reports are being used to monitor students browsing online which are checked by the headteacher/DSL

The challenge for DSLs and SLT is to better understand, review and drive the rationale behind decisions in this area. Tech teams and safeguarding teams will need to work much more closely together for this to be possible and technicians will be charged to carry out regular checks and feed back to DSL teams.

All staff need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via an email: TechSupport@stanboroughpark.herts.sch.uk, the contact form on the school website: <https://www.spsch.org/it-support/> or by coming to the IT Support office personally and will be asked for feedback at the time of the regular checks which will now take place.

Staff are reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

It is very important that schools understand the difference between filtering and monitoring, the meaning of overblocking and other terms, as well as how to get the best out of systems. There are guidance videos and flyers to help with this at <https://safefiltering.lgfl.net> and training is provided for all staff / safeguarding teams / technical teams as appropriate.

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

Messaging/commenting systems (incl. email, learning platforms & more)

Authorised systems

- Pupils at this school communicate with each other and with staff using emails provided by Microsoft 365. Only pre-approved external services (e.g. MOL NET+, Kerboodle, SparxMath, Makerbot, Practice Pal) are allowed to send emails to students. Students are using Google Classroom to communicate their homework and collaborate with each other. They are also using Kerboodle, SparxMath, Google Meet (students are able only to join sessions set by the school staff).
- Staff at this school use the email system provided by Microsoft 365 for all school emails. They are never to use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff are permitted to use this email system to communicate with everyone as long as it is work/school related.
- Staff at this school use Arbor to communicate with parents or with children, or with staff when concerning school/child data.
- Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the headteacher and centrally managed

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles

- More detail for all the points below are given in the Social media section of this policy as well as the school's acceptable use agreements, behaviour policy and staff code of conduct.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy found here: <https://www.spsch.org/policies/> and only using the authorised systems mentioned above.

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

- Pupils and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

Online storage or learning platforms

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc.

For all these, it is important to consider data protection and cybersecurity before adopting such a platform or service and at all times when using it. Stanborough Secondary School has a clear cybersecurity and data protection policy which staff, governors and volunteers must follow at all times.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher/Principal and Governors should ensure that this policy is updated to be in compliance with DfE stipulations. This policy once approved will be posted on the school web site.

The site is hosted by UK2.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – Sources must always be credited, and material only used with permission. If in doubt, check with the IT manager.

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For social media
- For a specific high-profile image for display or publication

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them)

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Stanborough Secondary School no member of staff should ever use their personal phone to capture photos or videos of pupils.

Photos are stored on a local network storage in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

Stanborough Secondary School works on the principle that if we don't manage our social media reputation, someone else will. Our Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first Googling the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

A member of the marketing team is responsible for managing our X-Twitter/Facebook/Instagram. Mrs J. Liburd and Mr D. Hopa manage our LinkedIn page.

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

Staff, pupils' and parents' Social Media presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school Complaints Procedure and Policy <https://www.spsch.org/policies/> should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school may need to deal with issues arising on social media involving pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the [Digital Family Agreement](#) to help establish shared expectations and the [Top Tips for Parents](#) poster along with relevant items and support available from parentsafe.lgfl.net and introduce the [Children's Commission Digital 5 A Day](#).

Although the school has an official Facebook / X-Twitter / Instagram / LinkedIn account and will respond to general enquiries about the school, it asks parents/carers not to use these channels, especially not to communicate about their children.

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

Pupils/students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a significant number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and video and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

The following sections on Device usage need to reflect current policies and any reviews or amendments to our policies to take into account the **balance** needed between filtering and monitoring to prevent access to harmful sites and care not to be over-blocking preventing student access to learning. We now have students who are part time and it is important that they use time between scheduled lessons productively. This may mean use of their own laptops and devices to access and process information. The rationale for arriving at policies for use of own devices e.g. only in years 10,11 needs to be stated and kept under review. Please complete this section to reflect updated policy.

Device usage

AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUPs and the sections of this document which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology and bring your own device (BYOD)

Please state school policy on use of personal laptops etc for personal study (Part time students may need to be considered)

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by the school of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD. Use of BYOD should not introduce vulnerabilities into existing secure environments and users should refer to the Acceptable Use Policy as well as Parental Information on Mobile Devices.

The following guidance provides some key points

- The school has a set of clear expectations and responsibilities for all users;
- The school adheres to the Data Protection Act 2008 and the General Data Protection Regulation (GDPR) principles;
- All users are provided with and accept the Acceptable Use Policy;
- All network systems are secure and access for users is differentiated;
- Where possible these (BYOD) devices will be covered by the school's normal filtering systems, while being used on the premises;
- All users will use their username and password and keep them safe;
- Pupils will receive training and guidance on the use of personal devices;
- Regular audits and monitoring of usage will take place to ensure compliance;
- Any device loss, theft, change of ownership of the device will be reported

Use of (BYOD) devices in the boarding school will be guided by Authorized Usage policies.

Pupils are allowed to bring mobile phones in for emergency use only / and may use mobile phones during lunch break, but not when moving around the school buildings. During lessons, phones must remain turned off at all times, unless the teacher has given express permission as part of the lesson. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the 'Digital images and video' section of this document and the school data protection cybersecurity policies. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

classrooms, and avoid capturing other children. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Use of school devices

Staff and pupils are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home.

School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct.

Wifi is accessible to staff, students and guests for school-related internet use/limited personal use within the framework of the acceptable use policy. All such use is monitored.

School devices for staff or students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable as well as appropriate personal use.

All and any usage of devices and/or systems and platforms may be tracked.

Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

The Arbor MIS system and parent groups on WhatsApp are used to communicate with parents.

Searching and confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools](#)', the Headteacher/Principal and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Full details of the school's search procedures are available in the school Behaviour Policy.

Appendix – Roles

Please read the relevant roles & responsibilities section from the following pages.

All school staff must read the “All Staff” section as well as any other relevant to specialist roles

Roles:

- All Staff
- Headteacher/Principal
- Designated Safeguarding Lead
- Governing Body, led by Online Safety / Safeguarding Link Governor
- CFL / RSHE Lead/s
- Computing Lead
- Subject / aspect leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Pupils
- Parents/carers
- External groups including parent associations

All staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current School e-Safety Policy and practices;
- they have read, understood and signed the School Staff Acceptable Use Policy (AUP);
- they report any suspected misuse or problem to the DSL for investigation/action/sanction;
- all digital communications with Pupils/parents/carers should be on a professional level and only carried out using official school systems;
- e-safety issues are embedded in all aspects of the curriculum and other activities;
- pupils understand and follow the e-safety and acceptable use policies;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor ICT activity in lessons, extra-curricular and extended school activities;
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices;
- in lessons where internet use is pre-planned 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.

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's main safeguarding policy, the code of conduct/handbook and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the designated safety lead as named in the Acceptable Usage Policy (AUP), maintaining an awareness of current online safety issues and

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

guidance (such as KCSIE 2025), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about overblocking, gaps in provision or pupils bypassing protections.

Headteacher

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead team ensuring they work with technical colleagues to complete an on-line safety audit in line with KCSIE 2025
- Has a duty of care ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety may be delegated to the e-Safety Coordinator
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure that ALL staff (including the e-safety Coordinator) undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles
- Receive regular monitoring reports from the e-safety coordinator and provide support for DSL and technical staff as they review safeguards.
- Be aware of the procedures to be followed in the event of a serious allegation made against a member of staff.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

- Understand the rationale behind decisions in filtering and monitoring as per the new DfE standards- in particular understand what is blocked or allowed for whom, when, and how as per KCSIE 2025. In liaison with the on-line safety governor.
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead / Online Safety Lead

Key responsibilities (remember the DSL can delegate certain online-safety duties but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

- The DSL should “take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place).
- The Designated Senior Lead should be trained in e-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 online contact with adults/strangers; potential or actual incidents of grooming and cyber-bullying.
- Be responsible for filtering and monitoring working closely with technical colleagues, SLT and the new “filtering” governor to learn more about this area, better understand, review and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home.
- Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL’s clear overarching responsibility for online safety is not compromised or messaging to pupils confused
- Ensure that ALL governors and trustees undergo safeguarding and child protection training (including online-safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online-safety and behaviour apply
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school) –
- Work with the headteacher, data protection officer (DPO) and governors to ensure a compliant framework for storing data, ensuring that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and “undertake Prevent awareness training.” – see safetraining.lgfl.net and prevent.lgfl.net
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

- Receive regular updates in online-safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples or sign up to the [LGfL safeguarding newsletter](#)
- Ensure that online-safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework ‘[Education for a Connected World – 2020 edition](#)’) and beyond, in wider school life
- Promote an awareness of and commitment to online-safety throughout the school community, with a strong focus on parents, including hard-to-reach parents – dedicated resources at parentsafe.lgfl.net
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine, e.g. a [survey to facilitate disclosures](#) and an online form on the school home page about ‘something that worrying me’ that gets mailed securely to the DSL inbox
- Pay particular attention to **online tutors**, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP,]

**Governing Body, led by Online Safety / Safeguarding Link Governor –
Key responsibilities (quotes are taken from Keeping Children Safe in Education)**

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) [Online safety in schools and colleges: Questions from the Governing Board](#)
- Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated –
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and headteacher to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring).

**CFL / RSHE Lead/s –
Key responsibilities:**

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the CFL / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives." [safetraining.lgfl.net]
- Focus on the underpinning knowledge and behaviours outlined in [Teaching Online Safety in Schools](#) in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress" – to complement the computing curriculum,.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within CFL/RSE.
- Note that an RSHE policy should be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Computing Lead – Mr Daniel Hopa

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject / aspect leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element

Network Manager/other technical support roles

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Note that KCSIE2023 changes expect a great understanding of technology and its role in safeguarding when it comes to filtering and monitoring and in 2023/4 you will be required to support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the new DfE standards, protections for pupils in the home and remote-learning.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / data protection officer / LGfL nominated contact / RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the data protection policy and cybersecurity policy are up to date, easy to follow and practicable
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Headteacher to ensure the school website meets statutory DfE requirements

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

Data Protection Officer (DPO) – Lorraine McDonald

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cybersecurity policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools, 2023*, “It’s not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child.” And in KCSIE 2025, “The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children.”
- Note that retention schedules for safeguarding records may be required to be set as ‘Very long-term need (until pupil is aged 25 or older)’. However, some local authorities require record retention until 25 for all pupil records. An example of an LA safeguarding record retention policy can be read at safepolicies.lgfl.net, but you should check the rules in your area.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors (including tutor)

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session**, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

Pupils

Key responsibilities:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they are expected to read, understand and sign before being given access to School systems;
- 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 e-safety practice when using digital technologies out of school and realize that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/carers

Key responsibilities:

- Read, sign and adhere to the school's parental acceptable use policy (AUP), read the pupil AUP and encourage their children to follow it
- Parents/Guardians should ensure that Pupils only access social networking sites in accordance with the published age restrictions of such sites.
- Parents are also responsible for monitoring their children's internet use and for ensuring that their children are not involved in any incidents of cyber-bullying. It is recognised that not all parents and careers may feel equipped to protect their son or daughter when they use electronic equipment at home hence the school organises occasions and age-appropriate information evenings for parents/guardians when a specialist offers advice about the potential hazards of this exploding technology, and the practical steps that parents/guardians can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm. The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents/guardians if there are any worries about a child or young person's behaviour in this area, and parents/guardians are encouraged to share any worries with us.
- Parents and guardians will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events; and on their children's personal devices in the school

External groups including parent associations –

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection

Stanborough School is committed to safeguarding and promoting the welfare of our pupils and expects all staff and volunteers to share this commitment. It is our aim that all our pupils fulfil their potential

- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

DRAFT