SHREWSBURY HOUSE SCHOOL TRUST

ONLINE SAFETY POLICY

Policy Owner:	Head of Trust IT
Approved by:	Designated Safeguarding Lead
Date of last review:	September 2025
Next review:	September 2026

1. Aims 2
2. Scope 2
3. Roles and Responsibilities 2
4. Education and Curriculum 3
5. Handling online-safety concerns and incidents 4
6. CCTV 7
7. Extremism 8
8. Data Protection and Cyber Security 8
9. Appropriate Filtering and Monitoring 8
10. Messaging / Commentating Systems (incl. email, learning platforms & more) 9
11. Use of Generative AI 11
12. Online Storage or Learning Platforms 11
13. School Website 12
14. Digital Images and Video 12
15. Social Media 12
16. Device Usage 14
Appendix A – Roles 17
All Staff 17
Executive Head / Head of TRS 17
Designated Safeguarding Lead (DSL) / Online Safety Lead 18
Governing Body, Designated Safeguarding Governor 20
PSHE & RSE – DSL 20
Computing Lead – Head of Trust IT 21
Subject Heads / Subject Leads and Heads of Departments 21
Head of Trust IT 21
Data Protection Lead – Bursar 22
Marketing - Registrar 23
Contractors 23
Pupils 23
Parents/Carers 23

1. Aims

This policy aims to promote a whole Shrewsbury House School Trust (SHST) approach to online safety by:

1.1. Setting out expectations for all SHST, (comprising Shrewsbury House School (SHS), and The Rowans School (TRS), community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).

1.2. 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. RSE \ PSHE) and beyond.

1.3. 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, and regardless of device or platform and that the same standards of behaviour apply online and offline.

1.4. Facilitate the safe, responsible and respectful 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.

1.5. Help SHST staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:

1.5.1. for the protection and benefit of the children and young people in their care;

1.5.2. for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice;

1.5.3. supporting the SHST ethos, aims and objectives, and protecting the reputation of the SHST and profession.

1.6. Establish 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 the Behaviour Management Policy or Anti-Bullying Policy).

2. Scope

This policy applies to all members of the SHST community (including staff, governors, contractors, 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.

3. Roles and Responsibilities

The SHST is a community and all members have a duty to behave respectfully online and offline 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 Trust. 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.

4. Education and Curriculum

Despite the risks associated with being online, SHST recognises the opportunities and benefits of children being online. Technology is a fundamental part of our adult lives and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

It is important that schools establish 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.

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, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

RSE and PSHE guidance also recommends schools assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress."

The following subjects have the clearest online safety links:

- Personal, Social, Health and Economic Education (PSHE)
- Relationships and Sex Education (RSE)
- Computing

However, as stated in Annex A, 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 or HODs, 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, generative AI tools, etc.) in school or setting as homework tasks, all staff should remind/encourage sensible use, monitor what pupils/students are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation and fake news), access to 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.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities

involving online technology, (including, co-curricular and extended school activities), supporting them with search skills, critical thinking (e.g. fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law.

An online safety audit is carried out annually and is a collaborative effort led by the Online Safety Lead.

5. Handling online-safety concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the safeguarding lead with any concerns (no matter how small these seem) to contribute to the overall picture or highlight what might not yet be a problem.

Support staff often have a unique insight and opportunity to find out about issues first in the playground, corridors, washrooms 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 (primarily in the first key document):

- Acceptable Use Policies (AUPs)
- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Management Policy
- Information Security Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc).

The SHST commits to take all reasonable precautions to safeguard 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. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead (OSL) / DSL on the same day – where clearly urgent, it will be made by the end of the lesson/club.

Any concern/allegation about staff misuse is always referred directly to the Executive Head for SHS or Head (TRS), unless the concern is about the Executive Head or Head (TRS) in which case the complaint is referred to the Chair of Governors and the LADO (Local
Authority's Designated Officer).

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer,

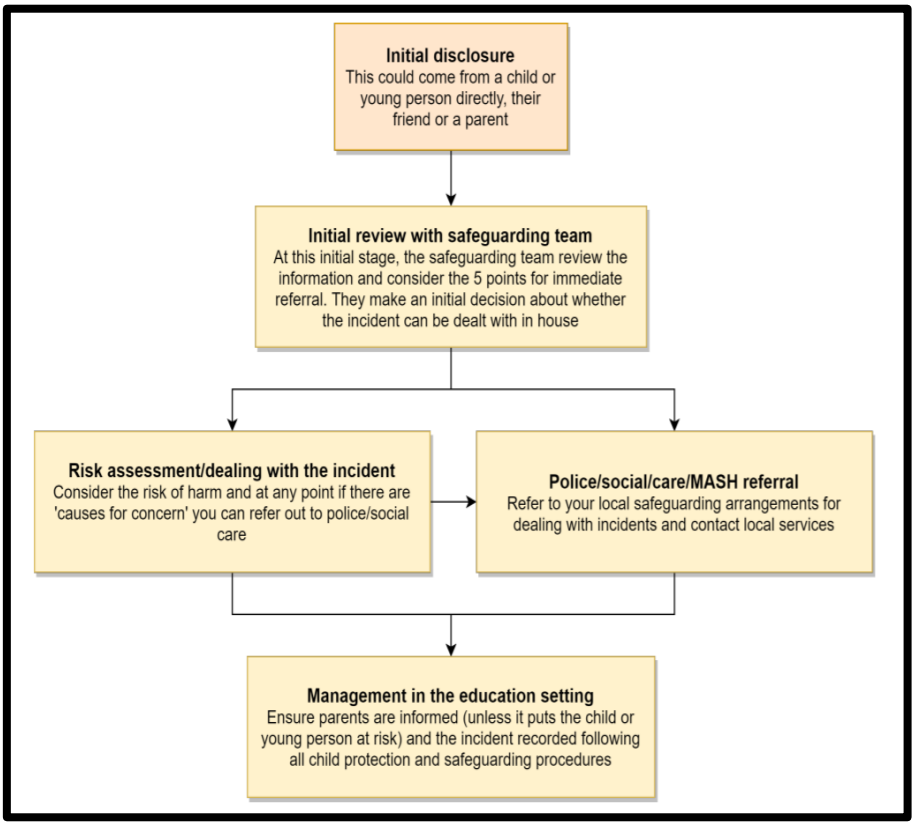
Police, IWF and Harmful Sexual Behaviour Support Service). The new DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 32-34 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

The following sub-sections provide detail on managing particular types of concern.

5.1. Nudes - sharing nudes and semi-nudes

All schools 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.

There is a one-page overview called Sharing nudes and semi-nudes: advice for education settings for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the DSL or OSL that first becomes 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.**



It is important that everyone understands that whilst the sharing of nudes involving children is illegal, students should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

The school DSL will 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 (see flow chart below from the UKCIS guidance) and next steps regarding liaising with parents and supporting pupils.

5.2. Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

5.3. Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed, (which may also be referred to as cyberbullying, including issues arising from banter).

It is important to be aware that sometimes fights are 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

5.4. Child-on-Child Sexual violence and 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.

5.5. 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 AUP 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 in the Information Security Policy and Data Protection Policy.

Where pupils contravene these rules, each School's Behaviour Management Policy will be applied; where staff contravene these rules, action will be taken as outlined in the SHST Staff Code of Conduct. 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.

5.6. Social Media Incidents

Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policies/social media policy/online safety.

Breaches will be dealt with in line with each school's Behaviour Management Policy (for pupils) or the SHST Staff 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, SHST 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.

6. CCTV

We use CCTV cameras to view and record individuals on and around the Trust's sites and on school transport in order to maintain a safe environment for pupils, staff and visitors, and to protect school property.

The CCTV system will not be used to:

- record sound
- for any automated decision taking; or
- monitoring private and/or residential areas or premises.

Before installing and using CCTV systems on our premises, we have:

- assessed and documented the appropriateness of and reasons for using CCTV;
- established and documented who is responsible for day-to-day compliance with this policy; and
- ensured signage is displayed to inform individuals that CCTV is in operation, and that CCTV operations are covered in appropriate policies.

CCTV monitors the Shrewsbury House School Site, The Rowans School site and Shrewsbury House Sports Ground. It is operational 24 hours a day and this data is continuously recorded.

Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example, to protect health and safety.

We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. This may include HR staff involved with disciplinary or grievance matters. Recorded images will only be viewed in designated, secure locations.

More detailed information on CCTV usage across SHST can be found in the Staff Handbook or on request.

7. Extremism

SHST has obligations relating to radicalisation and all forms of extremism under the UK Government's Prevent Duty guidance. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

8. Data Protection and Cyber Security

Please refer to the SHST's comprehensive policies.

9. Appropriate Filtering and Monitoring

The designated safeguarding lead (DSL) has lead responsibility for filtering and monitoring and works closely with the Online Safety Lead (OSL) to implement the DfE filtering and monitoring standards, which require schools to:

- 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.

We look to provide appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times. Filtering is provided by LGFL's SchoolProtect and monitoring by Securus.

We ensure ALL STAFF are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking.

Technical and safeguarding colleagues work together closely to carry out annual reviews and checks and also to ensure that the school responds to issues and integrates with the curriculum.

We carry out termly checks to ensure all systems are in operation, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc. More details of both documents and results are available on request dependent on staff roles from the OSL.

We use templates from LGfL for this documentation.

At SHST we recognise that generative AI sites can pose data risks so staff are not allowed to enter child data and where they use them, they must be approved. For children and young people, we

block the generative AI category and only allow specific sites. These are (Sparx Maths, Atom Learning and Century); we know that what children input and what the tool outputs cannot be guaranteed as safe and inappropriate content can be generated, so we carefully monitor output and limit their use - also in line with DfE guidelines. Find out more at genaisafe.lgfl.net

Safe Search is enforced on any accessible search engines on staff laptops and desktops and pupil Chromebooks and iPads.

Our YouTube moderate restricted mode is enforced for staff and strict restricted mode is enforced for all pupils.

When it comes to filtering the SHST uses LGFL's SchoolProtect. SchoolProtect allows devices to be filtered using HTTPS Decryption, IP addresses and usernames for both Windows and Chromebook devices. Different policies can be enabled which allows different filtering policies to be set up for staff, senior staff and pupils. Thus, Facebook, for example, can be blocked for staff and pupils but unblocked for senior staff.

The DSL checks SchoolProtect's Dashboard regularly and takes any necessary action as a result.

According to the DfE standards, "Your monitoring plan should include how you will monitor students when using school-managed devices connected to the internet." This may include:

- in-person monitoring in the classroom;
- device monitoring using device management software;
- network monitoring using log files of internet traffic and web access.

At SHST, we have decided that the first two options are appropriate. We have Securus 360 Full Monitoring Service to monitor teaching staff and pupils' use of Windows and Chromebooks. iPads are monitored through physical means. For TRS, due to the age of pupils, in-person monitoring of devices is the primary means of monitoring pupil activity.

Monitoring alerts are checked daily by the Securus Full Monitoring team and reports are sent to the DSL team, daily, weekly and monthly.

When pupils log into any school system on a personal device, activity may also be monitored here. For example, if you use your Google Workspace for Education account on a device at home.

10. Messaging / Commentating Systems (incl. email, learning platforms & more)

10.1. Authorised Systems

The school uses Gmail and SchoolBase as its main email systems. Gmail and SchoolBase are fully auditable, trackable and managed by the school. This is for the mutual protection and privacy of all staff, pupils and parents, safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

At SHS, Google Classroom is used for classwork and homework. The stream feature is turned off for pupils and teachers can provide feedback on work completed via the private comments feature which is available whenever an assignment is set but the teacher. For Reception, Year

1 and Year 2 pupils, Seesaw is used. Seesaw is also used predominantly at TRS.

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 OSL.

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 Executive Head or Head (TRS) (if by a staff member).

General principles for email (also see Behaviour Management Policy) use are as follows:

10.1.1. Email and VoIP are the only means of electronic communication to be used between staff and parents (in both directions).

10.1.2. Email to parents by staff may only be sent using the Trust email systems - SchoolBase for Parents and Gmail for all other emails. There should be no circumstances where a staff member's private email is used; if this happens by mistake, the DSL/Executive Head/ Head/Compliance Officer (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

10.1.3. Sensitive staff or pupil personal data should never be sent/shared/stored on email:

- If data needs to be shared with external agencies, Egress (secure email platform) will be used;
- Internally, staff should use the school network, including when working from home when remote access is available via the VPN system.

10.1.4. Pupils across the Trust do not have a school email which can be used to email others. At SHS, pupils do have an email account to log into Google Drive but this cannot be used for normal emailing. Pupils are not allowed to use private emails on any school IT device.

10.1.5. Staff may communicate to pupils to provide feedback for prep via Google Classroom.

10.2. Behaviour / Usage Principles of Messaging / Commenting Systems

10.2.1. 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.

10.2.2. 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.

10.2.3. Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.

11. Use of Generative AI

At SHST we acknowledge that generative AI platforms (e.g. ChatGPT or Gemini or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the DfE's guidance on this. In particular:

- We will talk about the use of these tools with pupils, staff and parents – their practical use as well as their ethical pros and cons.
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).
- The use of any generative AI in Exams, or to plagiarise and cheat is prohibited, and the Behaviour Policy will be used for any pupil found doing so.
- In school, we encourage pupils to not use AI platforms (such as ChatGPT) where they are underage. AI educational platforms (such as Sparks Maths, Atom Learning, Century etc.) which are approved by the school are used when deemed appropriate.
- Staff are encouraged to use AI to assist them with their teaching where appropriate.
- The Head of Digital Learning and Innovation will approve any AI platforms used in the curriculum.
- AI is covered thoroughly in the Computing curriculum where pupils are taught not just what AI and Machine Learning is but also the ethics of AI.
- Professional development courses and staff insets are used to upskill teachers in the use of AI in their teaching.

12. 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. Any new platforms will be approved by the OSL in consultation with SLT. The SHST has a clear Information Security policy and Data Protection policy which staff and governors must follow at all times.

13. School Website

Each school's website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The site is managed by / hosted by 'The Set UP'.

Where other staff submit information for the website, they are asked to remember:

- Schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published.

14. Digital Images and Video

How the SHST uses images and videos is outlined in each school's Taking, Storing and Using Images of Children Policy. It is vital that staff understand the differences in policy at EYFS and pupils in the older years. Refer to the Taking, Storing and Using Images of Children Policy for guidance here.

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

Staff and parents are reminded on all programmes of school events about the importance of not sharing without permission, due to reasons of child 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 computing lessons.

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 not to 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.

15. Social Media

15.1. Our SM presence

The SHST works on the principle that if we don't manage our social media reputation, someone else will.

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.

The Head of Trust Marketing is responsible for managing our X/Facebook/Instagram accounts and checking our Wikipedia and Google reviews and other mentions online.

15.2. Staff, pupils' and parents' SM presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a Trust, 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 Trust 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 Trust 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 Trust, 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 Trust's Complaints Procedure, found on each school's website, 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 Trust (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the Trust does deal with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms and not encourage or condone underage use. It is worth noting that online harms regulation is likely to require more stringent age verification measures over the coming years.

However, the Trust has to strike a balance of not encouraging under age use at the same time as needing to acknowledge reality in order to best help our pupils 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 do not 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). Further information can be found on Children's Commission Digital 5 A Day which gives easy to follow, practical steps for children and parents to achieve a healthy and balanced digital diet.

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

Email is the official electronic communication channel between parents and the school.

As outlined in the Acceptable Use Policies, pupils are not allowed to be 'friends' with or make a friend request to any staff, governors, and contractors or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, governor 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.

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 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.

16. 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.

16.1. Use of Personal Devices on Trust Sites

16.1.1. **Pupils** at SHS are allowed to bring mobile phones in for emergency use only and these must be handed in to the Senior Deputy Head on arrival at school. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to disciplinary action and the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, who will also pass on messages from parents to pupils in emergencies. Pupils are not allowed to have access to the school network or wireless network on their private devices.

16.1.2. **All staff who work directly with children** should never have their mobiles out or take calls when around pupils. The exception to this is where they are using them for school reasons such as taking photos which are to be used by the school. School data should never be downloaded onto a private phone. Staff should refer to the SHST's Information Security Policy and Staff Handbook (Bring your Own Device Policy), and the Taking, Storing and Using Images of Children Policy for more guidance.

16.1.3. **Contractors/governors** should leave their phones in their pockets and turn them 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 Head should be sought (the Executive Head or Head (TRS) may choose to delegate this) and this should be done in the presence of a member of staff.

16.1.4. **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 classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document.

16.1.5. Where **BYOD** is allowed, staff are not allowed to use a mobile hotspot to provide internet to the device as this would potentially bypass filtering in contravention of AUPs.

16.2. Use of School Devices

16.2.1. Staff and pupils are expected to follow the terms of the Trust's AUP for appropriate use and behaviour when on school devices, whether on site or at home.

16.2.2. School devices are not to be used in any way which contravenes AUPs, Behaviour Management policy /Staff Code of Conduct.

16.2.3. Wi-Fi is accessible to staff for school-related internet use / limited personal use within the framework of the AUP.

16.2.4. School devices for staff or pupils 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.

16.3. Trips/Events Away from School

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

16.4. Searching and Confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools]', the Executive Head or Head (TRS) 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.

Appendix A – Roles

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

School staff – note that you may need to read two sections – if your role is reflected here, you should still read the 'All Staff' section.

Roles:

- All Staff
- Executive Head / Head of TRS
- Designated Safeguarding Lead / Online Safety Lead
- Governing Body, led by Online Safety / Safeguarding Link Governor
- PSHE / RSE Leads
- Computing Lead
- Subject / Aspect Leaders
- Head of Trust IT
- Data Protection Lead
- Contractors
- Pupils
- Parents / Carers
- External groups including parent associations

All Staff

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

They must report any concerns, no matter how small, to the designated safety lead as named in the AUP, maintaining an awareness of current online safety issues (see the cover letter for issues in 2024) and guidance (such as KCSIE), 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 DfE standards for filtering and monitoring and play their part in feeding back to the DSL about overblocking, gaps in provision or pupils bypassing protections. All staff are also responsible for the physical monitoring of pupils' online devices during any session/class they are working within.

Executive Head / Head of TRS
Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the DSL to ensure that the DSL responsibilities listed in the section below are being followed and fully supported;

- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Ensure ALL staff 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
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with technical colleagues and the DSL–in particular understand what is blocked or allowed for whom, when, and how as per KCSIE. [LGfL's Safeguarding Shorts: Filtering for DSLs and SLT twilight provides an overview]
- Liaise with the DSLs or their deputies on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards
- Take overall responsibility for data management and information security ensuring that each individual school's provision follows best practice in information handling; work with the Compliance Officer, individual DSLs, their deputies and Governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that safeguarding and child protection is always put first and data-protection processes support careful and legal sharing of information
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead (DSL) / Online Safety Lead

Key responsibilities (remember the DSL can delegate certain online-safety duties, e.g. to the online-safety coordinator, 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).
- Ensure "An effective whole school approach" to online safety as per KCSIE.
- Ensure the school is complying with the DfE's standards on Filtering and Monitoring. [LGfL's Safeguarding Shorts: Filtering for DSLs and SLT twilight provides a quick overview and there is lots of information for DSLs at safefiltering.lgfl.net and appropriate.lgfl.net]
- As part of this, DSLs will work with technical teams to carry out reviews and checks on filtering and monitoring, to compile the relevant documentation and ensure that safeguarding and

technology work together. This will include a decision on relevant YouTube mode and preferred search engine/s etc.

- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- 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. RSE), 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 ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.
    - This must include filtering and monitoring and help them to understand their roles.
    - All staff must read KCSIE Part 1 and all those working with children also Annex B.
    - Cascade knowledge of risks and opportunities throughout the organisation.
- Liaise with the Executive Head and Chair of Governors to 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 online safety issues and be aware of the potential for serious safeguarding and child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.
- Remind staff of safeguarding considerations as part of a review of distance learning procedures and technology, including that the same principles of online safety and behaviour apply.
- Work with the Executive Head or Head (TRS), Compliance Officer and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that safeguarding and child protection is always put first and data-protection processes support careful and legal sharing of information.
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school).
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training."
- Review and update this policy, other online safety documents (e.g. AUP) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others).
- Receive regular updates in online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSE guidance and beyond, in wider school life.
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents.
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident 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/lockdown.
- 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, and those hired by parents.

Governing Body, Designated Safeguarding 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.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the DSL / OSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Work with the Compliance Officer, DSL and Executive Head / Heads 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.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B.
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring.
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school approach to online safety [with] a clear policy on the use of mobile technology."

PSHE & RSE – DSL
Key responsibilities:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships and Sex Education (RSE). "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."

- 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."
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE/RSE.
- Note that an RSE 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 – Head of Trust IT
Key responsibilities:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the RSE 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 the AUP.

Subject Heads / Subject Leads and Heads of Departments
Key responsibilities:

- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike.
- Ensure subject specific action plans also have an online-safety element.

Head of Trust IT
Key responsibilities:

- Collaborate regularly with the DSL and SLT to help them make key strategic decisions around the safeguarding elements of technology. Note that KCSIE changes expect a great understanding of technology and its role in safeguarding, so help DSLs and SLT to understand systems, settings and implications.
- Support safeguarding teams to understand and manage filtering and monitoring 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), 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 / online safety lead / data protection officer / LGFL nominated contact to ensure that school systems and networks reflect school policy.
- 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.
- Ensure filtering and monitoring systems work on new devices and services before releasing them to students and staff.
- 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, critical incident plans, and auditable access controls.
- 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.
- Ensure the data protection policy and cybersecurity policy are up to date, easy to follow and practicable. Network managers/technicians at LGFL TRUST net schools may want to ensure that you take advantage of the following solutions which are part of your package: Sophos Anti-Virus, Sophos Anti-Phish, Sophos Intercept X, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management. These solutions which are part of your package will help protect the network and users on it.
- Work with the Executive Head /Head (TRS) to ensure the school websites meet statutory DfE requirements.

Data Protection Lead – Bursar
Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support and ensure that the SHST Data Protection Policy and SHST Information Security Policy 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 2023, "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 <u>all</u> pupil records.

Marketing - Registrar
Key responsibilities:

- Work with the Executive Head or Head (TRS) to ensure the school website meets statutory DfE requirements.
- In conjunction with the DSL, approving any online security statements attached to communications such as emails and letters and addressing any online security queries.

Contractors
Key responsibilities:

- Read, understand, sign and adhere to the AUP.
- Report any concerns, no matter how small, to the DSL / OSL as named in the AUP.
- 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.

Pupils
Key responsibilities:

- Read, understand, sign and adhere to the pupil AUP.

Parents/Carers
Key responsibilities:

- Read, sign and promote the school's parental AUP and read the pupil AUP and encourage their children to follow it.