SUTTON GRAMMAR SCHOOL

ONLINE SAFETY POLICY

Staff member with responsibility:	Alex Marsh, Online Safety Lead
Reviewed by:	Board of Trustees
Policy Agreed date:	December 2022
Next review date:	December 2023

Contents

1. Introduction

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2022 (KCSIE) and other statutory documents; it is designed to sit alongside the school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

2. What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

The LGfL DigiSafe 2018 pupil survey of 40,000 pupils identified an increase in distress caused by, and risk from, content. For many years, online-safety messages have focused on 'stranger danger', i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced. Examples of this are the sharing of violent and sexual videos, self-harm materials, and coerced nudity via live streaming. Contact and conduct of course also remain important challenges to address.

3. How will this policy be communicated?

- Posted on the school website
- Available on the internal staff network/drive
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement.

4. Key Personnel

Ms Kate Ross	Deputy Head and Designated Safeguarding Lead (DSL)
Mr Alex Marsh	Online Safety Lead Head of Upper School and Deputy Designated Safeguarding Lead (DDSL)
Mr Chris Robson	Head of Lower School and DDSL
Mrs Lynda McDonald	Head of Year 13 and DDSL
Mr Tony Blunt	Head of P.E. and Games and DDSL
Mr Bob Murrill	Nominated Trustee for Safeguarding and Child Protection
Mr Ben Cloves	Headmaster
Mr Jeffrey Addy	Network Manager

5. Aims

This policy aims to:

- Set out expectations for all Sutton Grammar School's community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help 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
- 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

- Help 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
- Establish clear structures by which online behaviours 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)

6. Scope

This policy applies to all members of the Sutton Grammar School community (including 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.

7. 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.

7.1 Headteacher– Ben Cloves

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 and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Children Partnership (LSCP) guidance
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- 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 GDPR-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 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 cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- 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 that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory DfE requirements

7.2 Designated Safeguarding Lead & Online Safety Lead – Kate Ross & Alex Marsh
Quotations from KCSIE 2022
Key responsibilities:

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- 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
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the Headteacher, DPO and governors to ensure a GDPR-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.
- Stay up to date with the latest trends in online safety.
- 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.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- 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
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring
- 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 the 2019 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children Annex A
    - it would also be advisable for all staff to be aware of Annex C (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation

7.3 Governing Body, led by Safeguarding Link Governor – Bob Murrill
Key responsibilities (quotes are taken from Keeping Children Safe in Education 2020):

- Approve this policy and strategy and subsequently review its effectiveness
- "Ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of DSL [with] lead responsibility for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at governor meetings

- Work with the DPO, DSL and headteacher to ensure a GDPR-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 A; check that Annex C on Online Safety reflects practice in your school
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and are regularly updated in line with advice from the LSCP. Online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach."
- "Ensure appropriate filters and appropriate monitoring systems are in place but be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding". LGfL's appropriate filtering submission is **here**
- "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."

7.4 All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) is - Kate Ross
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – they may have discovered the missing piece so do not keep anything to themselves
- Sign and follow the staff acceptable use policy and code of conduct
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc.) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), 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
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions
- Use Senso to monitor student computer usage in computer rooms.
- Notify the DSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and any level of sexual harassment
- Be aware that they are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know
- Receive regular updates from the DSL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff and following the staff code of conduct.

7.5 Head of Personal Development – William Humphries

Key responsibilities from September 2020 (quotes taken from DfE press release on 19 July 2018 on New relationships and health education in schools):

As listed in the 'all staff' section, plus:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the Personal Development curriculum, "complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds."
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Personal Development

7.6 Computing Curriculum Lead – Sharon Corkery

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 DSL 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

7.7 Heads of Department

Key responsibilities:

As listed in the 'all staff' section, plus:

- Look for opportunities to embed online safety in their subject or aspect, and model positive attitudes and approaches to staff and pupils alike

7.8 Network Manager/technician – Jeffrey Addy

Key responsibilities:

As listed in the 'all staff' section, plus:

- 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 and data protection officer 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
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- 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
- 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

7.9 Data Protection Officer (DPO) – Neville Wrench

Key responsibilities:

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (April 2018), especially this quote from the latter document:
- GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place […] Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding
- The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'
- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above. You may be interested in the discounts for LGfL TRUSTnet schools for three market-leading GDPR compliance solutions at gdpr.lgfl.net
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

7.10 LGfL TRUSTnet Nominated contacts – Jeffrey Addy

Key responsibilities:

- To ensure all LGfL TRUSTnet services are managed on behalf of the school in line with school policies, following data handling procedures as relevant
- Work closely with the DSL and DPO to ensure they understand who the nominated contacts are and what they can do and what data access they have, as well as the implications of all existing services and changes to settings that you might request – e.g. for YouTube restricted mode, internet filtering settings, firewall port changes, pupil email settings, and sharing settings for any cloud services such as Microsoft Office 365 and Google Drive.
- Ensure the DPO is aware of the GDPR information on the relationship between the school and LGfL TRUSTnet at gdpr.lgfl.net

7.11 Volunteers and contractors

Key responsibilities:

- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator 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

7.12 Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student acceptable use policy and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media

- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

7.13 Parents/carers
Key responsibilities:

- Be aware of the Acceptable Use Policy signed by students
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible 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.

7.14 External groups including parent associations – SGS PTA
Key responsibilities:

- Support the school in promoting online safety and data protection
- 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

8. Education and curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):
Personal Development
Computing
Citizenship

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 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 are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), 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. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

Reviews of schemes of work (including for SEND pupils) are used as an opportunity to ensure delivery of key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

9. Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding.

General 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 err on the side of talking to the online-safety lead /

designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

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

Safeguarding and Child Protection Policy
Anti-Bullying Policy (Being updated)
Behaviour Policy (including school sanctions)
Acceptable Use Policy

Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc.)

Sutton Grammar School commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school and that those from outside school will continue to impact on 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 / 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 Headteacher 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.

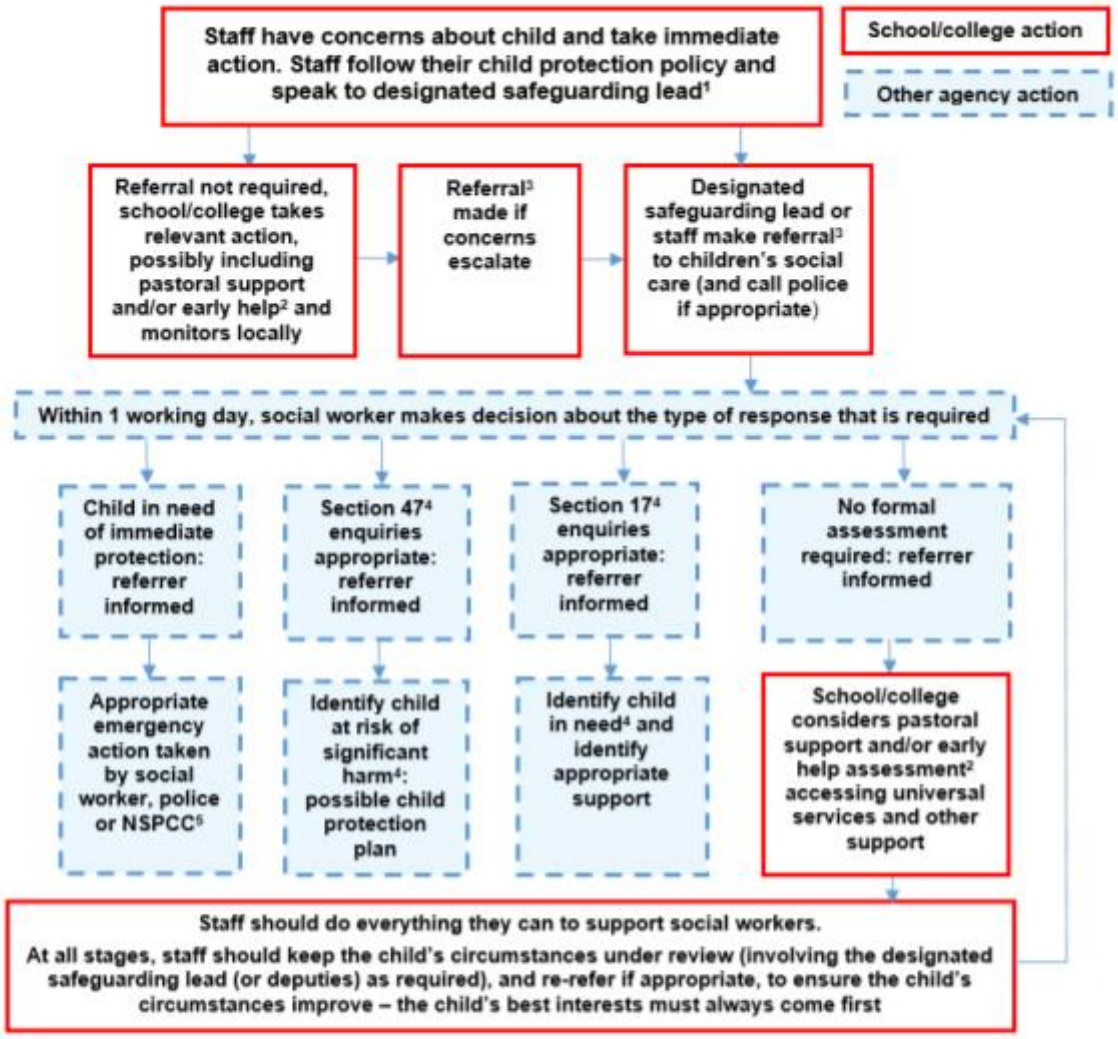
The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF).

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 disturbing or breaks the law (particular procedures are in place for youth produced sexual imaging; see section below).

10. Actions where there are concerns about a child

The following flow chart is taken from page 17 of Keeping Children Safe in Education 2020 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

Actions where there are concerns about a child



[1] In cases which also involve a concern or an allegation of abuse against a staff member, see Part Four of this guidance.

[2] Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working Together to Safeguard Children provides detailed guidance on the early help process.

[3] Referrals should follow the process set out in the local threshold document and local protocol for assessment. Chapter one of Working Together to Safeguard Children.

[4] Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Chapter one of Working Together to Safeguard Children.

[5] This could include applying for an Emergency Protection Order (EPO).

11. Youth produced sexual imaging

All schools (regardless of phase) should refer to the UK Council for Child Internet Safety (UKCIS) guidance on youth produced sexual imaging in schools. NB - where one of the parties is over 18, this is no longer youth produced sexual imaging but child sexual abuse.

There is a one-page overview 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) or online safety lead 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.

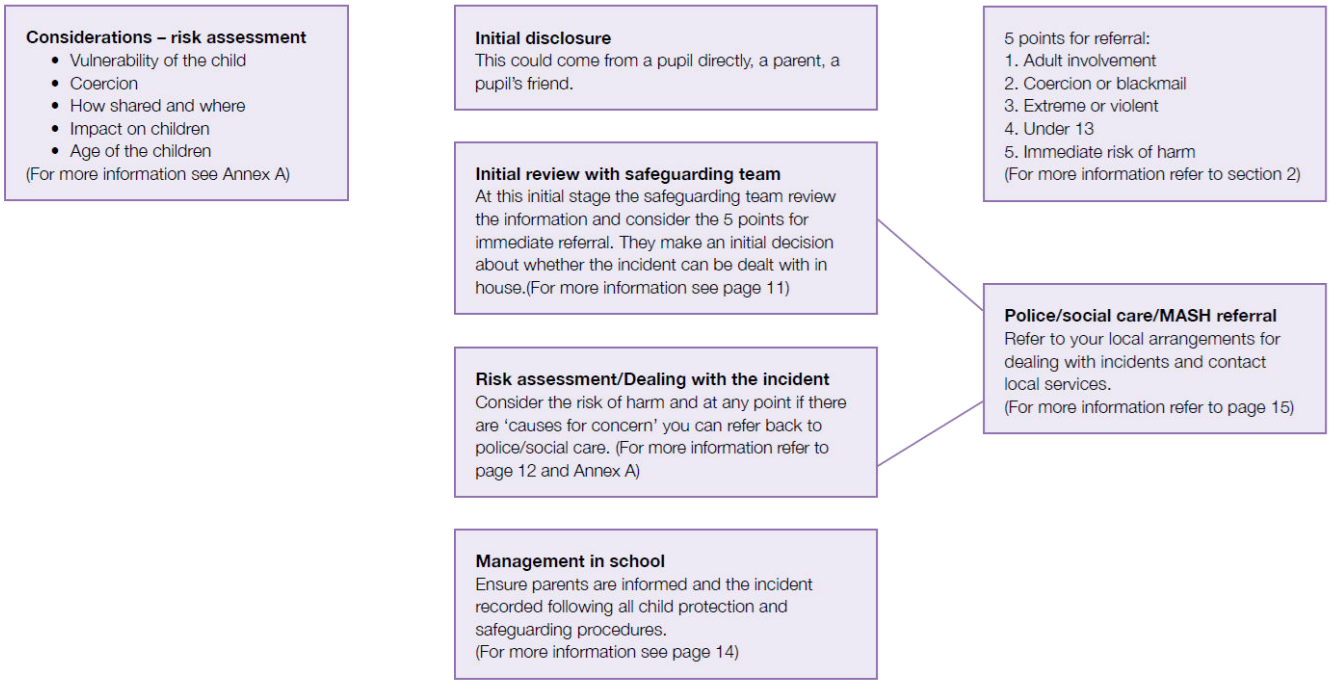
The school DSL will in turn use the full 50-page guidance document including case studies, typologies and a flow chart as shown below (for information only, must be viewed in the context of the full document) to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst youth produced sexual imaging 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.

The documents referenced above and materials to support teaching about youth produced sexual imaging can be found at youth produced sexual imaging.lgfl.net

Annex G

Flowchart for responding to incidents



12. Bullying

Online bullying 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. See anti-bullying policy.

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

13. 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. 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.

The following is an excerpt from section 56 on page 25 of that document:
"As with all safeguarding concerns, it is important that in such instances staff take appropriate action in accordance with their child protection policy. They should not assume that someone else is responding to any incident or concern. If in any doubt, they should speak to the designated safeguarding lead (or a deputy). In such cases, the basic safeguarding principles remain the same, but it is important for the school or college to understand why the victim has chosen not to make a report themselves. This discussion should be handled sensitively and with the support of children's social care if required. There may be reports where the alleged sexual violence or sexual harassment involves pupils or students from the same school or college, but is alleged to have taken place away from the school or college premises, or online.

There may also be reports where the children concerned attend two or more different schools or colleges.

The safeguarding principles, and individual schools' and colleges' duties to safeguard and promote the welfare of their pupils and students, remain the same. The same principles and processes as set out from paragraph 55 will apply. In such circumstances, appropriate information sharing and effective multi-agency working will be especially important."

14. 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 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.

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.

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.

15. Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Sutton Grammar School community. These are also governed by School Acceptable Use Policies. 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, Sutton Grammar 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 (run by the UK Safer Internet Centre) for support or help to accelerate this process.

16. Data protection and data security

This section serves to highlight general principles regarding the relationship between safeguarding and data protection / data security, and to signpost to useful information.

The Trust Board sets the framework to ensure compliance with the Data Protection Act 2018 and GDPR.

The Headmaster and data protection officer ensure a GDPR-compliant framework for storing data. Child protection is always put first and data-protection processes support careful and legal sharing of information.

The Trust's Data Protection policies and procedures can be found at https://www.suttongrammar.sutton.sch.uk/Data-Protection and in the Staff Handbook. The polices set out the Trust's legal basis for handling data.

The School's main provider of internet services is the London Grid for Learning Trust. Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection.
Information on the relationship between the School and LGfL Trust can be found at https://www.lgfl.net/gdpr/default.aspx

There are useful links and documents to support schools with data protection in the 'Resources for Schools' section of that page but you should first read the Trust's polices and consult the Trust's DPO, DSL or the Headmaster if you have any concerns.

The Department for Education's 'Keeping Children Safe in Education 2022' states:

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 promote the welfare and protect the safety of children.

Governing bodies and proprietors should ensure relevant staff have due regard to the data protection principles, which allow them to share personal information, as provided for in the Data Protection Act 2018 and the GDPR.

Relevant staff should be confident of the processing conditions under the Data Protection Act 2018 and the UK GDPR which allow them to store and share information for safeguarding purposes, including information which is sensitive and personal, and should be treated as 'special category personal data'. Schools should not under the UK GDPR as supplemented by the Data Protection Act 2018 provide pupils' education data where the serious harm test under that legislation is met. Therefore, in a situation where a child is in a refuge, this could mean that schools can withhold education data under the GDPR; they should do so where the serious harm test is satisfied.

Governing bodies and proprietors should ensure that staff who need to share 'special category personal data' are aware that the Data Protection Act 2018 contains 'safeguarding of children and individuals at risk' as a processing condition that allows practitioners to share information. This includes allowing practitioners to share information without consent, if it is not possible to gain consent, it cannot be reasonably expected that a practitioner gains consent, or if to gain consent would place a child at risk.

Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding."

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. Emails sent to external authorities regarding students should be encrypted in accordance with the requirements of the receiving organisation. Normally the DSL will be responsible for authorising this communication.

Staff must not use privately owned devices to hold or transmit personal data of staff or students. Data must only be managed and sent using the School's devices and networks. Unauthorised disclosure or use of confidential information will be a breach of the Trust's Employee Rules.

17. Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At this Sutton Grammar School, the internet connection is provided by LGfL TRUSTnet. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen, which is made specifically to protect children in schools. You can read more about why this system is appropriate on the UK Safer Internet Centre's appropriate filtering submission pages here.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

- Physical monitoring (adult supervision in the classroom, at all times)
- Internet and web access
- Active/Pro-active technology monitoring services

At Sutton Grammar School, we have decided that option 3 is appropriate and we will use Senso to monitor computer usage in school. We also have Senso picking up any searches or phrases students use that may be a concern regarding an individual's health or well-being. Further information regarding Senso can be found at the following link.

18. Email

Pupils at this school use the LondonMail system from LGfL TRUSTnet for all school emails.
Staff at this school use the StaffMail for all school emails.

Both these systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL TRUSTnet on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email is the main means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Other platforms will involve Microsoft Teams and Show My Homework. Use of a different platform must be approved in advance by the data-protection officer / Headteacher. 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).

- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
- If data needs to be shared with external agencies, USO-FX and Egress (from Sept 2018) systems are available from LGfL TRUSTnet.
- Internally, staff should use the school network, including when working from home when remote access is available via the Freedom2Roam system.
- There is no restriction applied to student's emails.
- 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
- Pupils and staff are allowed to use the email system for reasonable 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.
- See also the social media section of this policy.

19. 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 and Governors have delegated the day-to-day responsibility of updating the content of the website to Simeon Brook, Assistant Head.

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

- School 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. There are many open-access libraries of high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this site). Pupils and staff at LGfL TRUSTnet schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

20. Cloud platforms

Many schools are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning.

This school adheres to the principles of the Department for Education document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'.

As more and more systems move to the cloud, it becomes easier to share and access data. It is important to consider data protection before adopting a cloud platform or service.

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush –never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The data protection officer and network manager analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought

- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

21. 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 and for what purpose (beyond internal assessment, which does not require express consent). Parents answer as follows:

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

Whenever a photo or video is taken, the member of staff taking it will check the latest database before using it for any purpose. See Safeguarding Policy and Staff Code of Conduct for how these images should be taken.

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).

All staff are governed by their contract of employment and the school's code of conduct, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Sutton Grammar School, no member of staff will ever use their personal phone to capture photos or videos of pupils unless in exceptional circumstances.

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

Staff and parents are reminded 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.

Staff 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. Staff 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. Staff teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

22. Social media

Sutton Grammar School works on the principle that if the school doesn't manage its 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.

All staff are responsible for managing our varying social media accounts. They must complete the Social Media request form (Appendix I) before each academic year

23. 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 school, we accept that many parents, staff and pupils will use it. However, as stated in the Staff Code of Conduct or the Student Acceptable Use Policy, 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 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 or 16, but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to ensure their children respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

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).

Email is the official electronic communication channel between parents and the school, and between staff and pupils (see page 15 for full details) and Satchel: One in the case of homework.

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.

Students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). 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, 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.

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.

24. Device usage

Please read the following in conjunction with acceptable use policies and staff code of conduct and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

25. Personal devices and bring your own device (BYOD) policy

Students in the sixth form are allowed to bring mobile phones in and may use mobile phones during lunch break or in sixth form only areas, 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 confiscation and sanctions in line with the Behaviour Policy and 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.

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 classrooms, and avoid capturing other children. For school events, parents should refer to the Digital images and video section of this document on page 17. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

26. Network / internet access on school devices

Students are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.

Volunteers, contractors, governors can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

Parents have no access to the school network or wireless internet on personal devices.

27. Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number is used for any authorised or emergency communications with pupils 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.

28. Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher 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.

29. Policy Review

This policy will be reviewed by the DSL and Online Safety Lead in December 2023.

30. Appendices

A. Personal Development Coverage of E-Safety
B. Computer Science Coverage of E-Safety
C. Acceptable Use Policies (AUPs) for Students
D. Safeguarding Policy
E. Safeguarding Concern Form
F. Behaviour Policy
G. Anti-Bullying Policy (to be updated)
H. Staff Code of Conduct
I. Social Media Request Form