ST IVO ACADEMY
Astrea Academy Trust
INSPIRING BEYOND MEASURE

Online Safety Policy

Adopted: September 2023
Next review due: September 2025

What is this policy?

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

Aims

This policy aims to:

- Set out expectations for all St Ivo Academy 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 misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour/Anti-Bullying policy)

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 students identified an increase in distress caused by, and risk from, content. For many years, online-safety messages have focussed 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. This survey can be found here: **studentsurvey.lgfl.net**

Further Help and Support

Internal school channels will be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with the Astrea Academy Trust Safeguarding Policy. The DSL or DDSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and the Principal or DSL will handle referrals to the LA designated officer (LADO).

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both students and staff, including the Professionals’ Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

Scope

This policy applies to all members of the St Ivo Academy community (including staff, LECC committee members, volunteers, contractors, students, 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.

This policy can only impact upon practice if it is a living document, accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff drive – projects/staff/policies
- Available in paper format in the office
- All staff (teaching and non teaching) asked to confirm they have read and understood the policy using the Athena system.
- Integral to safeguarding updates and training for all staff (especially in September refreshers)

Roles and responsibilities

KCSIE makes clear that “the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)”. As such, St Ivo Academy’s online safety coordinator is Laura Brasher, the Designated Safeguarding Lead.

That said, the 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, students, families and the reputation of the school.

Principal

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 Board (LSCB) 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 LGC members 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 students, 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 LGC members are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory DfE requirements

Designated Safeguarding Lead / Online Safety Lead

Key responsibilities

The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).

- Ensure an effective approach to online safety that empowers the school to protect and educate the whole school 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 Principal, DPO and LGC 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 and the strategy on which it is 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 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 LGC link member to discuss current issues (anonymised), review incident logs and discuss appropriate follow up action.
- 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
- Oversee and discuss 'appropriate filtering and monitoring' with the LGC, both physical and technical and ensure staff are aware
- Ensure the latest 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, including that all staff must read KCSIE Part 1 and all those working with children Annex A

Online Safety / Safeguarding Link LECC member

Key responsibilities:

- Note this policy and strategy and subsequently review its effectiveness
- 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 LGC meetings
- Work with the DPO, DSL and Principal 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

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) and Online Safety Lead (OSL) is

- Read Part 1 and Annex A 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 – you may have discovered the missing piece so do not keep anything to yourself
- Read, understand and follow the staff code of conduct (Guidance for Safer Working Practice). Notify the DSL/OSL if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for students)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide students 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 students to follow the Acceptable Use Policy, remind them about it and respond to incidents appropriately,
- Notify the DSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you 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. More guidance on this point can be found in this Online Reputation guidance for schools.

Personal Development Lead

Key responsibilities from September 2022 (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 (PSHE / RSE) 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 and approaches within Personal Development

Subject leaders

Key responsibilities:

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

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

Central IT Team – including named individuals supporting at St Ivo Academy

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 / online safety lead / data protection officer to ensure that school systems and networks reflect school and trust 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)
- Be responsible for the implementation of 'appropriate filtering and monitoring'
- 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

Data Protection Officer (Trust DPO) and Academy Data Protection Lead

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, Principal and LGC to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited in line with the Astrea Academy Trust Data Protection Policy.

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

Students

Key responsibilities:

- Understand and adhere to the student Acceptable Use Policy and review this periodically
- 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
- 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

Parents/carers

Key responsibilities:

- Read the student Acceptable Use Policy and encourage their children to follow it
- 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 school staff, volunteers, LGC members, contractors, students or other parents/carers.

Education and curriculum

The following subjects have the clearest online safety links: Personal Development and Computing

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

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting, all staff should encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide students 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.

Handling online safety concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding as well as being a curriculum strand, PSHE theme and the integral part of the revised, statutory Relationships and Sex Education policy.

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 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 Policy
Behaviour Policy
Anti-bullying Policy
Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
Guidance for Safer Working Practice (which acts as the staff code of conduct)

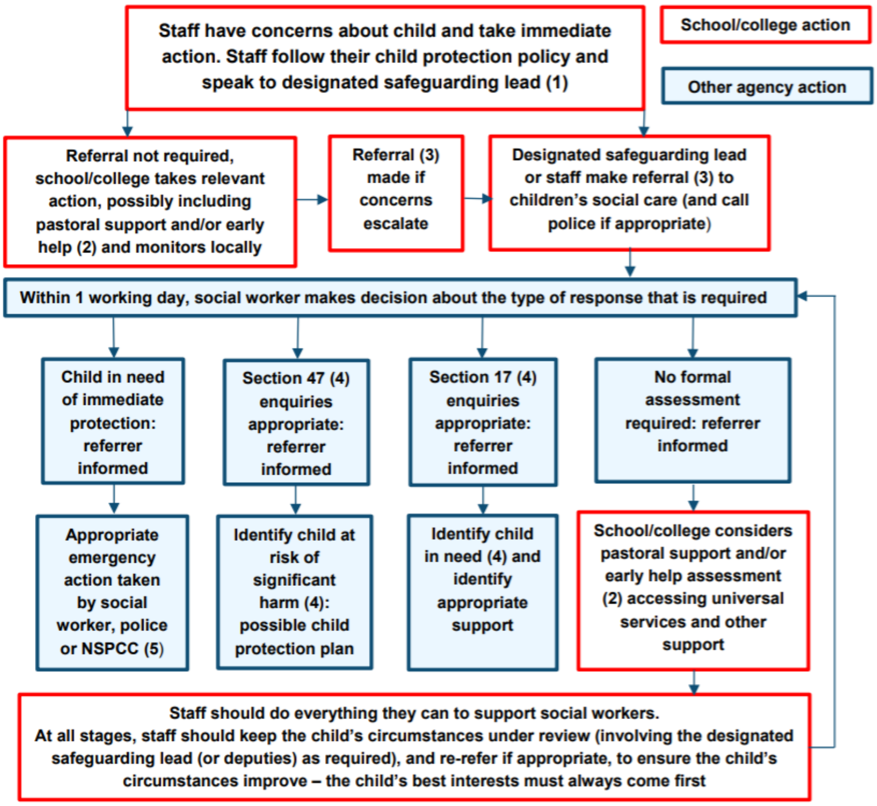
The school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on students when they come into school). All members of the school are encouraged to 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 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 Principal, unless the concern is about the Principal in which case the allegation is referred to the trust Head of safeguarding and Chief Operating Officer. Staff may also use Astrea’s Whistleblowing policy.

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 students engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting; see section below).

Actions where there are concerns about a child

The following flow chart is taken from page 16 of Keeping Children Safe in Education 2022 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.


Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead (1)
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help (2) and monitors locally
Referral (3) made if concerns escalate
Designated safeguarding lead or staff make referral (3) to children's social care (and call police if appropriate)
Within 1 working day, social worker makes decision about the type of response that is required
Child in need of immediate protection: referrer informed
Section 47 (4) enquiries appropriate: referrer informed
Section 17 (4) enquiries appropriate: referrer informed
No formal assessment required: referrer informed
Appropriate emergency action taken by social worker, police or NSPCC (5)
Identify child at risk of significant harm (4): possible child protection plan
Identify child in need (4) and identify appropriate support
School/college considers pastoral support and/or early help assessment (2) accessing universal services and other support
Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

(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).

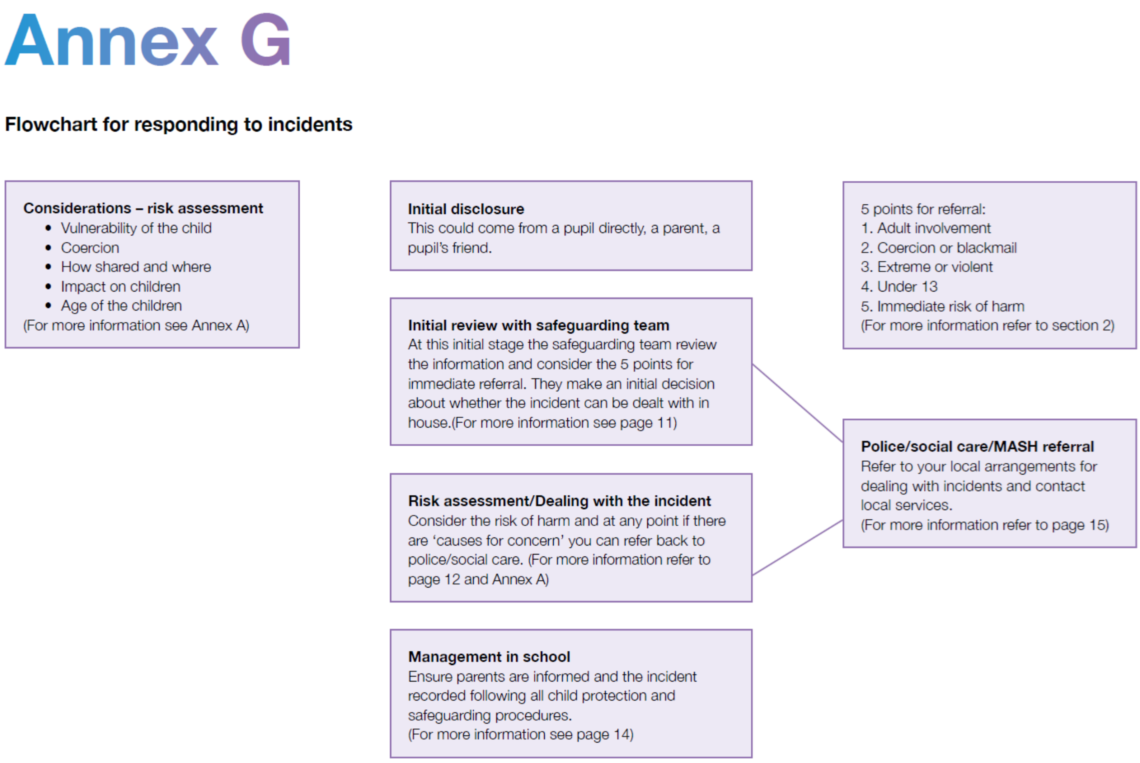
Sexting

We work to the UK Council for Child Internet Safety (UKCCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting 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) to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document including 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 sexting is illegal, students/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 sexting can be found at sexting.lgfl.net



Annex G

Flowchart for responding to incidents

Considerations – risk assessment
- Vulnerability of the child
- Coercion
- How shared and where
- Impact on children
- Age of the children

(For more information see Annex A)

Initial disclosure
This could come from a pupil directly, a parent, a pupil's friend.

Initial review with safeguarding team
At this initial stage the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house.(For more information see page 11)

Risk assessment/Dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you can refer back to police/social care. (For more information refer to page 12 and Annex A)

Management in school
Ensure parents are informed and the incident recorded following all child protection and safeguarding procedures.
(For more information see page 14)

5 points for referral:
1. Adult involvement
2. Coercion or blackmail
3. Extreme or violent
4. Under 13
5. Immediate risk of harm

(For more information refer to section 2)

Police/social care/MASH referral
Refer to your local arrangements for dealing with incidents and contact local services.
(For more information refer to page 15)

Bullying

Online bullying should be treated like any other form of bullying and the behaviour and anti-bullying policies should be followed for online bullying, which may also be referred to as cyberbullying. Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Sexual violence and harassment

In 2022 new Department for Education guidance was issued on sexual violence and harassment, as a new section within Keeping Children Safe in Education and also a document in its own right.

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.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern student 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/code of conduct as well as in this policy, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices, and other technology**.**

Where students contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, this will be managed by the Principal. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in St Ivo Academy community. These are also governed by acceptable Use policies and Guidance for Safer Working Practice (staff). Breaches will be dealt with in line with the school behaviour policy (students) or disciplinary policy (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, St Ivo Academy 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.

Data protection and data security

There are 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), which the DPL and DSL will seek to apply. This quote from the latter document is useful for all staff:
“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 .”

All students, staff, LECC members, volunteers, contractors and parents are bound by the school’s data protection policy and agreements, which can be found here.

The Principal, data protection officer and LGC members work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

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**.**

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place, they should 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 St Ivo Academy, we have a dedicated and secure connection that is protected with firewalls and multiple layers of security, including a web filtering system called Smoothwall.

Electronic communications

Email

Staff and students at this school use Microsoft Office 365 for all school emails.
General principles for email use are as follows:

- Email is the only means of electronic communication to be used between staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer / Principal in advance. 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 Principal (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/Principal/DPL (the

particular circumstances of the incident will determine whose remit this is) should be informed immediately

- Staff or pupil personal data should not normally be sent/shared/stored on email.
    - If data needs to be shared with external agencies, this is to be encrypted or password protected.
    - Internally, staff should use the school network, including when working from home when remote access is available
    - 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
    - Staff should not use the email system for personal use and 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.

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 Principal has delegated the day-to-day responsibility of updating the content of the website to the Director of School Strategic Operations.

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

- St Ivo Academy has 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 student 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 students's full name).

Cloud platforms

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

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. St Ivo Academy uses Microsoft Office 365.

For online safety, basic rules of good password hygiene, expert administration and training can help to keep staff and students safe, and to avoid incidents. The central IT team analyses and documents systems and procedures before they are implemented, and regularly reviews 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, in consultation with the trust Head of IT, what may or may not be stored in them and by whom.
- 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
- Students 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
- Student images/videos are only made public with parental permission
- Only school approved platforms are used by students or staff to store student work
- All stakeholders understand the difference between consumer and education products (e.g. a private account and those belonging to a managed educational domain)

Digital images and video

When a 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 use, which does not require express consent).

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

Any students 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 Guidance for Safer Working Practice document which acts as the code of conduct. Photos and videos are stored on the school network or on Microsoft Office 365 in line with Astrea's Data Protection Policy.

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).

Students are taught about how images can be manipulated in their online safety education programme.

Students 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.

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

Social media

St Ivo Academy’s Social Media presence

The school has a number of whole school and department/year group social media channels. There are whole school accounts for Facebook, Instagram and Twitter. Management of these accounts is the responsibility of the Director of School Strategic Operations.

Management of department/year accounts is the responsibility of an identified individual, with oversight from the Director of School Strategic Operations. Such accounts may be public or private dependent of usage and purpose. Creation of any accounts must be discussed with the Director of School Strategic Operations prior to implementation.

Staff, students’ and parents’ Social Media 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 students will use it. However, 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 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 by email 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, students and parents, also undermining staff morale and the reputation of the school (which is important for the students we serve).

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. 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 students/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). It is encouraging that 73% of students (from the 40,000 who answered that LGfL DigiSafe pupil online safety survey) trust their parents on online safety (although only half talk about it with them more than once a year at the moment).

Students are not allowed* to be ‘friends’ with or make a friend request** to any staff, LGC member, volunteer and contractor or otherwise communicate via social media.

Students are discouraged from ‘following’ staff, LECC member, volunteer or contractor public accounts (e.g. following a staff member with a public professional Twitter 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 Principal, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Principal (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 or trust, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that of the 131 Prohibition Orders issued to staff in 2017, 73 involved social media/technology (and 27 of the 66 orders by August 2018).

Device usage

Personal devices and bring your own device (BYOD) policy

Students are allowed to bring mobile phones in to school but they should not be used, seen or heard during the school day.
All staff who work directly with children should leave their mobile phones on silent. Certain staff require access to their mobile phone to access school email information during the school day. Child/staff data should never be downloaded onto a private phone.
Volunteers, contractors, LGC members should not under any circumstance use personal devices 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 a member of SLT and this should be done in the presence of a member of 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. Parents are asked not to call students on their mobile phones during the school day; unless requested to do so by staff, urgent messages can be passed via the school office.

Network / internet access on school devices

Students (except Sixth Form) do not have access to Wi-Fi whilst in the school setting.
Volunteers, contractors, LECC members can access the guest wireless network but have no access to networked files/drives. All internet traffic is monitored.
Parents have no access to the school network or wireless internet on personal devices

Trips / events away from school

For school trips/events away from school, and extended curriculum teachers using their personal phone will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number. Staff can have TEAMS on their personal mobile phones which allows them to call from their personal phone through the school office number. Direct dial numbers can also be setup on request, or staff can use the designated trips mobile.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Principal and staff authorised by them have a statutory power to search students/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.