Online-Safety Policy

Parallel Learning Trust
A Multi-Academy Trust

Introduction

Key people / dates

Sutton House Academy	Designated Safeguarding Lead (DSL) team	Mrs R Wyatt Mr E Muca Miss N Ayres Miss S Dutton Miss L Stephens
	Online-safety lead (if different)	
	Academy Council Online-safety / safeguarding link	Anne Sturman
	PSHE/RSHE lead	Neve Ayres
	Network manager / other technical support	Matt Tisley
	Date this policy was reviewed and by whom	August 2025, Neve Ayres
	Date of next review and by whom	August 2026

What is this policy?

Online safety is an integral part of safeguarding and requires a whole academy, cross-curricular approach and collaboration between key academy leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2024 (KCSIE), 'Teaching Online Safety in Schools 2024' and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside the academy's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the academy's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the academy and local area. Although many aspects will be informed by legislation and regulations, staff, Academy Council Members, pupils and parents will be

involved in writing and reviewing the policy (KCSIE stresses making use of teachers' day-to-day experience on the ground). This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Pupils could help to design a version in language their peers understand, or help you to audit compliance. The academy's Acceptable Use Policies for different stakeholders will help with this are also reviewed alongside this overarching policy. Any changes to this policy is immediately disseminated to all the above stakeholders.

Who is in charge of online safety?

The above person is in charge of online-safety at your academy; this person is also the Designated Safeguarding Lead and takes lead responsibility for safeguarding and child protection (including online safety).

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 academy response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

Many of these new risks are mentioned in KCSIE 2024, e.g. fake news, upskirting and sticky design. To keep yourself updated with prominent new and emerging trends, follow safeblog.lgfl.net.

LGfL's 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 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.

How will this policy be communicated?

This policy is a living document (regularly updated) that is accessible and understood by stakeholders. This document will be communicated in the following ways:

- Posted on the academy website
- Available on the internal staff network/drive
- Available in paper format in the staffroom
- Part of academy 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)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole academy community, on entry to the academy, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- AUPs are displayed in appropriate classrooms/corridors (not just in Computing corridors/classrooms)
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

Online-Safety Policy

Parallel Learning Trust
A Multi-Academy Trust

Contents

Introduction 1
Key people / dates 1
What is this policy? 1
Who is it for; when is it reviewed? 1
Who is in charge of online safety? 2
What are the main online safety risks today? 2
How will this policy be communicated? 2
Contents 4
Overview 6
Aims 6
Further Help and Support 6
Scope 7
Roles and responsibilities 7
Headteacher Mr E Muca 7
Designated Safeguarding Lead / Online Safety Lead –Mrs R Wyatt 8
Academy Council , led by Online Safety / Safeguarding Link Academy Council Member – Anne Sturman 9
All staff 10
PSHE / RSHE Lead/s – Neve Ayres 12
Computing Lead – SLT 12
Subject / aspect leaders 12
Network Manager/technician – Matt Tisley 13
Data Protection Officer (DPO) 14
LGfL TRUSTnet Nominated contacts – Matt Tisley 14
Volunteers and contractors 15
Pupils 15
Parents/carers 15

External groups including parent associations 16
Education and curriculum 16
Handling online-safety concerns and incidents 17
Actions where there are concerns about a child 19
Sexting 21
Upskirting 22
Bullying 22
Sexual violence and harassment 22
Misuse of academy technology (devices, systems, networks or platforms) 22
Social media incidents 23
Data protection and data security 24
Appropriate filtering and monitoring 25
Electronic communications 26
Email 26
Academy website 27
Cloud platforms 27
Digital images and video 28
Social media 29
Staff, pupils' and parents' SM presence 30
Device usage 32
Personal devices including wearable technology and bring your own device (BYOD) 32
Network / internet access on academy devices 32
Trips / events away from academy 33
Searching and confiscation 33
Review of the Digital and Technology Standards 33

Online-Safety Policy

Parallel Learning Trust
A Multi-Academy Trust

Overview

Aims

This policy aims to:

- Set out expectations for all Sutton House 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 academy gates and academy 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 academy 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 academy, supporting the academy ethos, aims and objectives, and protecting the reputation of the academy 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 academy policies such as Behaviour Policy or Anti-Bullying Policy)

Further Help and Support

Internal academy channels should always be followed first for reporting and support, as documented in academy policy documents, especially in response to incidents, which should be reported in line with your Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the headteacher will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC 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.

Online-Safety Policy

Parallel Learning Trust
A Multi-Academy Trust

Scope

This policy applies to all members of the Sutton House Academy 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, or who use technology in their academy role.

Roles and responsibilities

This academy 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 academy, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the academy. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Headteacher Mr E Muca

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-academy 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 Partnerships
- Liaise with the Designated Safeguarding Lead on all online-safety issues which might arise and receive regular updates on academy issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the academy'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 academy implements and makes effective use of appropriate ICT systems and services including academy-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 Academy Council members are regularly updated on the nature and effectiveness of the academy's arrangements for online safety
- Ensure the academy website meets statutory requirements

Designated Safeguarding Lead / Online Safety Lead –Mrs R Wyatt

Key responsibilities (remember the DSL can delegate certain online-safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2024):

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). The DSL will need to work more closely with the IT team, but this is safeguarding driven and NOT technology driven (A Safeguarding First approach).
- 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 the academy to protect and educate the whole academy 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 – the new LGfL DigiSafe **pupil survey** of 40,000 pupils may be useful reading (new themes include 'self-harm bullying' and getting undressed on camera)
- 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 academy trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter
- Ensure that online safety education is embedded across the curriculum (e.g. by use of the UKCIS framework 'Education for a Connected World') and beyond, in wider academy life
- Promote an awareness and commitment to online safety throughout the academy community, with a strong focus on parents, who are often appreciative of academy support in this area, but also including hard-to-reach parents
- Liaise with academy technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss 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
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are aware (Ofsted inspectors have asked classroom teachers about this). The academy uses LGfL filtering, the filtering statement can be viewed at https://saferinternet.org.uk/guide-and-resource/teachers-and-academy-staff/appropriate-filtering-and-monitoring/filtering-provider-responses
- Ensure the 2018 DfE guidance on sexual violence and harassment is followed throughout the academy 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
    - cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more

Academy Council , led by Online Safety / Safeguarding Link Academy Council Member – Anne Sturman

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2024):

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- "Ensure an appropriate **senior member** of staff, from the academy 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 academy in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at Academy Council meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- 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 academy 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 academy
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated […] in line with advice from the local three safeguarding partners […] integrated, aligned and considered as part of the overarching safeguarding approach." There is further support for this at cpd.lgfl.net
- "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 (https://saferinternet.org.uk/guide-and-resource/teachers-and-academy-staff/appropriate-filtering-and-monitoring/provider-responses)
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole academy approach to online safety [with] a clear policy on the use of mobile technology." NB – you may wish to refer to 'Teaching Online Safety in Schools 2024' and investigate/adopt the UKCIS cross-curricular framework 'Education for a Connected World' to support a whole-academy approach

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) are Mrs R Wyatt.
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the academy's main safeguarding policy

- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with academy 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
- Sign and follow the staff acceptable use policy and code of conduct/handbook
- Notify the DSL/OSL if policy does not reflect practice in your academy and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all academy activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in academy or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended academy 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
- Prepare and check all online source and resources before using within the classroom
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce academy sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment (your DSL will disseminate relevant information from the new DfE document on this)
- 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/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues – you may find it useful to read at least the headline statistics and conclusions from the LGfL DigiSafe pupil survey (https://www.lgfl.net/online-safety/hopesandstreams) of 40,000 pupils (new themes include 'self-harm bullying' and getting undressed on camera)
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the academy hours and site, and on social media, in all aspects upholding the reputation of the academy and of the professional reputation of all staff.

PSHE / RSHE Lead/s – Neve Ayres

responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.

Computing Lead – SLT

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/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in academy to ensure a common and consistent approach, in line with acceptable-use agreements

Subject / aspect leaders

Key responsibilities:

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

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

Network Manager/technician – Matt Tisley

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Keep up to date with the academy's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact to ensure that academy systems and networks reflect academy 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 academy's online security and technical procedures
- To report online-safety related issues that come to their attention in line with academy policy
- Manage the academy'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
- Network managers/technicians take advantage of the following LGFL solutions which are part of the package: Sophos Anti-Virus, Sophos Anti-Phish (from Sept 2024), Sophos InterceptX, Sophos Server Advance, Egress (from Sept 2024), Meraki Mobile Device Management. These solutions which are part of the LGFL package that will help protect the network and users on it
- Monitor the use of academy technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with academy policy

Data Protection Officer (DPO)

Key responsibilities:

- NB – this document is not for general data-protection guidance; GDPR information on the relationship between the academy and LGfL can be found at gdpr.lgfl.net; there is an LGfL document on the general role and responsibilities of a DPO in the 'Resources for Schools' section of that page
- 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 academies' (August 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. Lawful and secure information sharing between academys, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant 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."

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)'. However, some local authorities require record retention until 25 for all pupil records. An example of an LA safeguarding record retention policy can be read at safepolicies.lgfl.net, but you should check the rules in your area.

- Work with the DSL, headteacher and Academy Council 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.

LGfL TRUSTnet Nominated contacts – Matt Tisley

Key responsibilities:

- To ensure all LGfL services are managed on behalf of the academy in line with academy 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 / 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 G Suite.

- Ensure the DPO is aware of the GDPR information on the relationship between the academy and LGfL at gdpr.lgfl.net

Volunteers and contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / 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

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil 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 academy and realise that the academy's acceptable use policies cover actions out of academy, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at academy or outside academy if there are problems

Parents/carers

Key responsibilities:

- Read, sign and promote the academy's pupil acceptable use policy (AUP) along with their children and encourage them to follow it

- Consult with the academy if they have any concerns about their children's and others' 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 academy staff, volunteers, governors, contractors, pupils or other parents/carers.
- NB: the LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety (but only half talk about it with them more than once a year).

External groups including parent associations

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within academy
- Support the academy 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 academy staff, volunteers, governors, contractors, pupils or other parents/carers

Education and curriculum

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

- PSHE
- Relationships education, relationships and sex education (RSE) and health
- 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 academy activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in academy or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended academy 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.

At Sutton House Academy, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCIS (the UK Council for Internet Safety.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its 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.

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 of Computing, PSHE/RSHE and Citizenship.

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.

Support 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).

Academy 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
- Sexual Harassment / Peer on Peer Abuse Policy (if separate)
- Anti-Bullying Policy
- Behaviour Policy (including academy sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This academy commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside outside the academy (and that those from outside the academy will

continue to impact on pupils when they come into the academy).All members of the academy are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the academy's escalation processes.

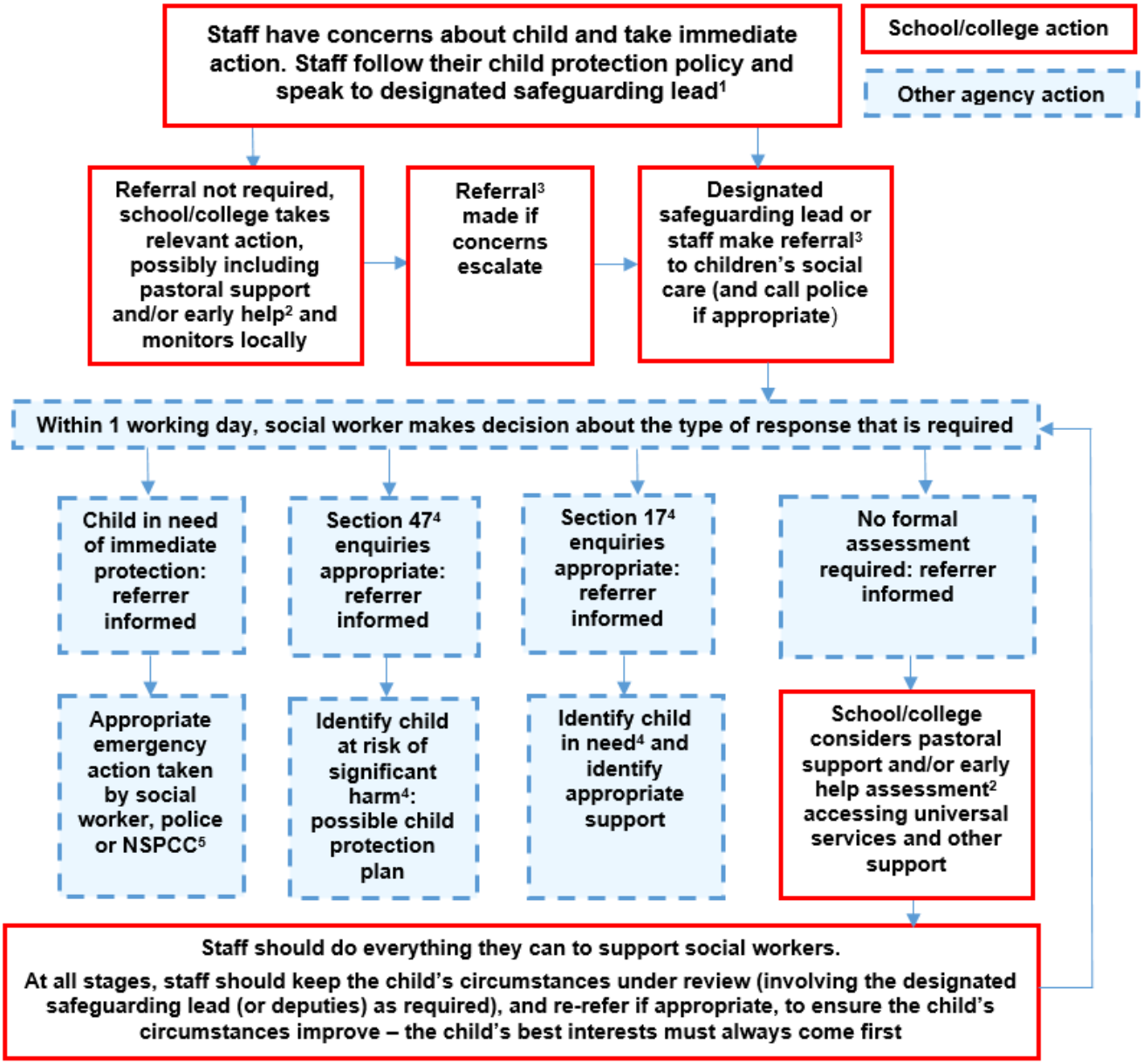
Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson. This should also be reported to IT Support in order to start an investigation.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Executive Headteacher/Interim CEO and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC 50 Helpline (you may want to display a poster with details of this / other helplines in the staff room – see posters.lgfl.net and reporting.lgfl.net).

The academy 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 sexting and upskirting; see section below).

Actions where there are concerns about a child

The following flow chart (it cannot be edited) is taken from page 22 of Keeping Children Safe in Education 2024 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



[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. See Working Together to Safeguard Children for further guidance
[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

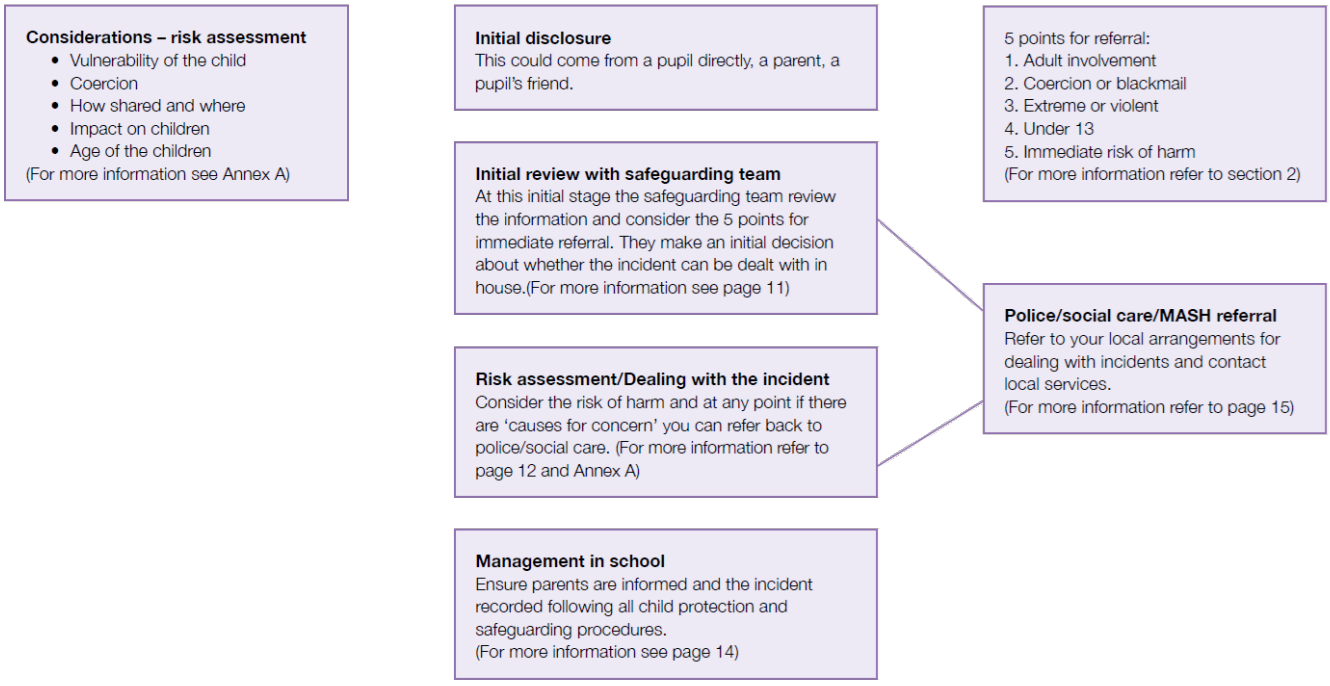
All academies (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in academys. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sexting; how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) 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 academy DSL will in turn use the full guidance document, Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk) to decide next steps and whether other agencies need to be involved.

Annex G

Flowchart for responding to incidents



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

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

Upskirting

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

Bullying

Online bullying should be treated like any other form of bullying and the academy bullying policy 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

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. It would be useful for all staff to be aware of this guidance: paragraphs 468-471 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

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 academies 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 academy technology (devices, systems, networks or platforms)

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

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 academy platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

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

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

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Sutton House Academy community. These are also governed by academy Acceptable Use Policies and the academy social media policy.

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

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the academy community, Sutton House 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 academy 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

GDPR information on the relationship between the academy and LGfL can be found at gdpr.lgfl.net; there are useful links and documents to support academys with data protection in the 'Resources for Academys' section of that page.

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' (September 2024), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

"**GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.** Lawful and secure information sharing between academys, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in academies are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant 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**."

All pupils, staff, governors, volunteers, contractors and parents are bound by the academy's data protection policy and agreements. Further, this academy makes use of the following discounted GDPR solution from LGfL:

- GDPR Sentry

Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: USO sign on for LGfL services, Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Egress and Meraki Mobile Device Management.

The headteacher, data protection officer, Academy Council and IT team 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. The use of [USO-FX / Egress] to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

The academy's data-protection documentation covers/or should cover these areas:

- CCTV
- Use of personal vs academy devices
- Password policy / two-factor authentication
- Reminders to lock devices when leaving unattended
- Device encryption
- Access to and access audit logs for academy systems
- Backups
- Security processes and policies
- Disaster recovery
- Access by third parties, e.g. IT support agencies
- BYOD
- Wireless access
- File sharing
- Cloud platform use, access and sharing protocols

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges academies to "ensure appropriate filters and appropriate monitoring systems are in place [and] 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 academy, the internet connection is provided by LGfL. This means we have a dedicated and secure, academysafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in academies. You can read more about why this system is appropriate on the UK Safer Internet Centre's appropriate filtering submission pages.

https://saferinternet.org.uk/guide-and-resource/teachers-and-academy-staff/appropriate-filtering-and-monitoring/provider-responses

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

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

At Sutton House Academy, we have decided that all the above options are appropriate and have recently deployed Impero software to connect and protect staff and students on any device on the academy network.

Electronic communications

Please read this section alongside references to pupil-staff communications in the overall academy Safeguarding Policy, and in conjunction with the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

Email

- Pupils at this academy have the ability to use the LondonMail / PupilMail system from LGfL for all academy emails
- Staff at this academy use the StaffMail system for all academy emails

Both these systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL on behalf of the academy. 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 only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer / headteacher 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 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 (the particular circumstances of the incident will determine whose remit this is) 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 systems are available from LGfL. The academy's MS Office365 OneDrive can also be used.
    - Internally, staff should use the academy network, including when working from home when remote access is available via the RAV3 system gateway or Cisco Anyconnect VPN.
- Pupils are restricted to ONLY receive emails from trusted domains and cannot email external accounts
- 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 academy into disrepute or compromise the professionalism of staff
- Pupils are NOT allowed to use the email system for 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.

- Staff are Not allowed to the email system for personal use, emails are not monitored but should be aware 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. Access maybe granted by LGFL to staff emails to assist with ongoing investigation of misconduct or/and police investigation.

See also the social media section of this policy.

Academy website

The academy website is a key public-facing information portal for the academy community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Academy Council have delegated the day-to-day responsibility of updating the content of the website to Sutton House Academy. The site is managed / hosted by Schudio.

The DfE has determined information which must be available on a academy website. LGfL has compiled RAG (red-amber-green) audits at safepolicies.lgfl.net to help academys to ensure that requirements are met (see appendices).

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

- Academies have the same duty as any person or organisation to respect and uphold copyright law – academies have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. If in doubt, check with Matt Tisley. 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 academys 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).

Cloud platforms

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

This academy adheres to the principles of the DfE document 'Cloud computing services: guidance for academy leaders, academy 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. Cloud platforms used at the academy are: Microsoft's Office 365, Google for Education's G Suite, myDrive for file storage and Adobe Cloud.

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
- Pupil images/videos are only made public with parental permission
- Only academy-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)

Digital images and video

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

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

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

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

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

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

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. Further detail on this subject and a sample letter to parents for taking photos or videos at academy events can be found at parentfilming.lgfl.net

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

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

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

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

Social media

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

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the academy online). Few parents will apply for an academy

place without first 'googling' the academy, and the Ofsted pre-inspection check includes monitoring what is being said online (Mumsnet is a favourite).

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 academys' (and staff members') online reputation.

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

Eve Glennister/Janine Willet are responsible for managing our Twitter/Facebook. They follow the guidance in the LGfL / Safer Internet Centre online-reputation management document .

(https://static.lgfl.net/LgflNet/downloads/online-safety/LGfL-OS-Advice-Online-Reputation-Managment-for-Academys.pdf)

Staff, pupils' and parents' SM presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a academy, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the academy community sign, we expect everybody to behave in a positive manner, engaging respectfully with the academy 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 academy 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 academy, 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 academy 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 academy (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the academy regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms 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 academy 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 academy the next day). You may wish to introduce the Children's Commission Digital 5 A Day. (https://www.childrenscommissioner.gov.uk/our-work/digital/5-a-day)

The academy has an official Facebook / Twitter (managed by Eve Glennister and will respond to general enquiries about the academy, but asks parents/carers not to use these channels to communicate about their children.

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

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

Pupils/students are discouraged from 'following' staff, Academy Council, 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.

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 academy 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 academy or its stakeholders on social media and be careful that their personal opinions might not be attributed to the academy, trust or local authority, bringing the academy into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there have been 200 Prohibition Orders issued to teachers over the past four years related to the misuse of technology/social media.

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

Device usage

Please read the following in conjunction with acceptable use policies 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.

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

- **Pupils/students** are allowed to bring mobile phones in for emergency use only but must hand in the phones to the academy office as they enter the academy building. Important messages and phone calls to or from parents can be made at the academy office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during academy hours. See also the Digital images and video section on page 28 and Data protection and data security section on page 24. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the academy office to answer on their behalf or ask for the message to be left with the academy office.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at academy events, please refer to the Digital images and video section of this document on page 28. Parents are asked not to call pupils on their mobile phones during the academy day; urgent messages can be passed via the academy office.

Network / internet access on academy devices

- **Pupils/students** are NOT allowed networked file access via personal devices and are not allowed to connect to the academy's wifi network.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during academy hours. See also the Digital images and video section

on page 28 and Data protection and data security section on page 24. Child/staff data should never be downloaded onto a private phone.

- **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 academy network or wireless internet on personal devices. All internet traffic is monitored.

Trips / events away from academy

For academy trips/events away from academy, teachers will be issued a academy duty phone/tablet and this number used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the academy 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.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for academys', the Headteacher/Principal and staff authorised by them have a statutory power to search pupils/property on academy 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 academy's search procedures are available in the academy Behaviour Policy.

Review of the Digital and Technology Standards

We work in line with the DfE Digital and Technology Standards Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK (www.gov.uk) and review these standards twice a year.