

## Introduction

### Key people / dates

	Designated Safeguarding Lead (DSL) team	Helen Currie, Lindsay Read, Pat English, Naline Sabaroche, Sarah Davies, Rockena Muirhead
	Online-safety lead (if different)	Helen Currie
	Online-safety / safeguarding link governor	Mark Brown
	PSHE/RSHE lead	n/a
	Network manager / other technical support	Hasina Rashid/Sean McLean
	Date this policy was reviewed and by whom	14/10/21, Alison Emmett
	Date of next review and by whom	September 2022

### What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with ‘Keeping Children Safe in Education’ 2021 (KCSIE), ‘Teaching Online Safety in Schools’ 2019, statutory RSHE guidance 2019 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 your school’s statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school’s safeguarding and child protection procedures. **At FANS we follow the Early Years Foundation Stage Curriculum (EYFS), which was rewritten for September 2021.**

### Who is it for; when is it reviewed?

This policy should be a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. We recommend you read the **DfE ‘[Get help with remote education](#)’** guidance at [safepolicies.lgfl.net](http://safepolicies.lgfl.net) before reissuing your school policies for online safety, safeguarding and AUPs to see what needs changing in the light of potential closure, remote learning and alternative arrangements at school. Although many aspects will be informed by legislation and regulations, you should involve staff, governors, pupils and parents 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. Acceptable Use Policies (see appendices) for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

### Who is in charge of online safety?

You may have a named online-safety lead at your school (see above); this person may or may not be the designated safeguarding lead (DSL), but **KCSIE makes clear that “the designated safeguarding lead should take 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 school 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 2021, e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual exploitation, criminal exploitation, serious youth violence, upskirting and sticky design.

In past and potential future **remote learning and lockdowns**, there is a greater risk for grooming and exploitation (CSE, CCE and radicalisation) as children spend more time at home and on devices. There is a real risk that some of your pupils may have missed opportunities to disclose such abuse during the lockdowns or periods of absence. The quick audit [safeposters.lgfl.net](https://safeposters.lgfl.net) or quiz at [digisafedigest.lgfl.net](https://digisafedigest.lgfl.net) may help to surface some of these issues.

Following the government's investigation into **peer-on-peer sexual abuse** and [Ofsted review](#), schools will need to review their policies to ensure appropriate processes are in place to allow pupils to report sexual harassment and abuse concerns freely, knowing these will be taken seriously and dealt with swiftly and appropriately – ensure pupils are aware of the new [NSPCC helpline](#) and your school’s internal reporting channels. Ways we can help you stay up to date with the latest news, risks, opportunities, best-practice and trends include the LGfL DigiSafe [blog](#), [newsletter](#) and our [Twitter](#)/[Facebook](#) channels.

### How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be 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 network/drive
- Available in paper format in the staffroom
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- 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 school community, on entry to the school, 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) **and on the school website**
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

## Contents

**NB – don't edit the names or otherwise update this page; edit the titles in the relevant section. This table will then automatically update when you save/exit; if not, click on the table below and press F9.**

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/Principal – <b>Helen Currie</b>	7
Designated Safeguarding Lead / Online Safety Lead – <b>Helen Currie</b>	8
Governing Body, led by Online Safety / Safeguarding Link Governor – <b>Mark Brown</b>	10
All staff	11
PSHE / RSHE Lead/s – <b>Pat English/Nalinee Sabaroche</b>	12
Computing Lead – <b>Helen Currie</b>	13
Subject / aspect leaders	13
Network Manager/technician – <b>Sean McLean</b>	13
Marketing & Policy Officer – <b>Alison Emmett</b>	14
Data Protection Officer (DPO) – <b>Maryline Avis</b>	14
LGfL TRUSTnet Nominated contacts – <b>Helen Currie, Hasina Rashid, and Sean McLean (SSC)</b>	15
Volunteers and contractors (including tutor)	16
Children	16
Parents/carers	16

External groups including parent associations – Friends of FANS	17
Education and curriculum	17
Handling online-safety concerns and incidents	18
Actions where there are concerns about a child	19
Sexting – sharing nudes and semi-nudes	21
Upskirting	22
Bullying	22
Sexual violence and harassment	22
Misuse of school technology (devices, systems, networks or platforms)	22
Social media incidents	23
Data protection and data security	23
Appropriate filtering and monitoring	26
Electronic communications	26
Email	26
School website	27
Cloud platforms	28
Digital images and video	28
Social media	29
FANS’ SM presence	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 school devices	33
Trips / events away from school	33
Searching and confiscation	33
Appendices	34

## Overview

### Aims

This policy aims to:

- Set out expectations for all **FANS** 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, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- 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 Policy or Anti-Bullying Policy)

### Further Help and Support

Internal school channels should always 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 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](https://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 new NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

## Scope

This policy applies to all members of the **FANS** community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

## Roles and responsibilities

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

## Headteacher/Principal – Helen Currie

### Key responsibilities:

- Support safeguarding leads and technical staff as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards (see [remotesafe.lgfl.net](https://remotesafe.lgfl.net) for policy guidance and an infographic overview of safeguarding considerations for remote teaching technology).
- 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 Partnerships
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements (see appendices for website audit document)

### Designated Safeguarding Lead / Online Safety Lead – Helen Currie

**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 2021):

- “The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] ... this **lead** responsibility should not be delegated”
- Work with the HT and technical staff to review protections for **pupils in the home** e.g. DfE **Umbrella scheme** or **LGfL HomeProtect filtering for the home** and **remote-learning** procedures, rules and safeguards (see [remotesafe.lgfl.net](https://remotesafe.lgfl.net) for guidance to policies and an infographic overview of safeguarding considerations for remote teaching technology.
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure “An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.”
- “Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs, or the named person with oversight for SEN in a college and Senior Mental Health Leads) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies.”
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns

- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Work 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 safeguarding and “undertake Prevent awareness training.” – see [safetraining.lgfl.net](https://safetraining.lgfl.net) and [prevent.lgfl.net](https://prevent.lgfl.net)
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends – see [safeblog.lgfl.net](https://safeblog.lgfl.net) for examples or sign up to the [LGfL safeguarding newsletter](https://lgflsafeguardingnewsletter.com)
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework ‘[Education for a Connected World – 2020 edition](https://www.gov.uk/guidance/education-for-a-connected-world-2020-edition)’) and beyond, in wider school life. **At FANS we follow the EYFS curriculum for PSED to ensure that we support young children’s well-being.**
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, but also including hard-to-reach parents – dedicated resources at [parentsafe.lgfl.net](https://parentsafe.lgfl.net)
- 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 how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine/lockdown, e.g. a safe, simple, online form on the school home page about ‘something that worrying me’ that gets mailed securely to the DSL inbox/
- Oversee and discuss ‘appropriate filtering and monitoring’ with governors (is it physical or technical?) and ensure staff are also aware (Ofsted inspectors have asked classroom teachers about this). Are you talking to your technical teams? Whilst they will do the technical work, key decisions on what should be allowed are the responsibility of the DSL who should be careful to keep children safe but “be careful that ‘over blocking’ does not lead to unreasonable restrictions” (KCSIE). [Our Safeguarding Shorts: Filtering for DSLs and SLT](https://www.gov.uk/guidance/our-safeguarding-shorts-filtering-for-dsls-and-slt) twilight provides a quick overview.
- Ensure the updated [2021 DfE guidance on Sexual Violence & Sexual Harassment Between Children in Schools & Colleges](https://www.gov.uk/guidance/2021-dfe-guidance-on-sexual-violence-and-sexual-harassment-between-children-in-schools-and-colleges) Guidance is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying.
- Facilitate training and advice for all staff, including supply teachers:

- all staff must read KCSIE Part 1 and all those working with children Annex B – translations are available in 12 community languages at [kcsietranslate.lgfl.net](https://kcsietranslate.lgfl.net)
- Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
- it would also be advisable for all staff to be aware of Annex D (online safety)
- cascade knowledge of risks and opportunities throughout the organisation
- [cpd.lgfl.net](https://cpd.lgfl.net) has helpful CPD materials including PowerPoints, videos and more
- Pay particular attention to **online tutors** this year, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP, and those hired by parents - share [the Online Tutors – Keeping Children Safe](#) poster at [parentsafe.lgfl.net](https://parentsafe.lgfl.net) to remind parents of key safeguarding principles

### Governing Body, led by Online Safety / Safeguarding Link Governor – **Mark Brown**

#### Key responsibilities (quotes are taken from Keeping Children Safe in Education 2021)

- 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](#)
- Ask about how the school has reviewed protections for **pupils in the home** (including when with online tutors) and **remote-learning** procedures, rules and safeguards (see [remotesafe.lgfl.net](https://remotesafe.lgfl.net) for guidance to policies and an infographic overview of safeguarding considerations for remote teaching technology.
- “Ensure an appropriate **senior member** of staff, from the school or college **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support...”
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor 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 school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B; check that Annex D on Online Safety reflects practice in your school
- “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](https://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](#)
- “Ensure that children are taught about safeguarding, including online safety [...] as part of providing a broad and balanced curriculum [...] Consider a whole school or college 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 2019’ and investigate/adopt the UKCIS cross-curricular framework ‘Education for a Connected World – 2020 edition’ to support a whole-school approach

### All staff

#### Key responsibilities:

- In 2021 pay particular attention to safeguarding provisions for **home-learning** and **remote-teaching technologies** (see [remotesafe.lgfl.net](https://remotesafe.lgfl.net) for an infographic overview of safeguarding considerations for remote teaching technology. There are further details in the staff AUP.
- Recognise that **RSHE** is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject. **FANS recognise this but follow the EYFS curriculum for this age group.**
- 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 **Helen Currie**
- Read Part 1, Annex B and Annex D of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex B for SLT and those working directly with children, it is good practice for all staff to read all three sections). Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
- 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

- Sign and follow the staff acceptable use policy and code of conduct/handbook:  
<H:\POLICIES & PROCEDURES\Safeguarding\e-safety policies\e-safety 2021-22>  
<H:\POLICIES & PROCEDURES\HR - Personnel, Term & Conditions, JD's etc\Code of conduct>
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, 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 in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place)
- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the [remotesafe.lgfl.net](https://remotesafe.lgfl.net) infographic which applies to all online learning.
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using
- Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL/OSL of new trends and issues before they become a problem
- **In 'Getting Along Together' we promote speaking kindly to each other. We do this in person and online.**
- 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 safeguarding 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.

**PSHE / RSHE Lead/s – Pat English/Naline Sabaroche**

### Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSED/ 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 technology Understanding the World curriculum, where children only use technology with adult support and are not left online unattended. If an adult is modelling searching for information, they discuss only doing this with an adult present.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should now be included on primary and secondary school websites.

### Computing Lead – Helen Currie

#### Key responsibilities:

- As listed in the 'all staff' section, plus:
- FANS follow the EYFS curriculum for Understanding the world, technology.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

### Subject / aspect leaders

#### Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the new RSHE curriculum, 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 Schools can be applied in your context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element

### Network Manager/technician – Sean McLean

#### Key responsibilities:

- As listed in the 'all staff' section, plus:
- Support the HT and DSL team as they review protections for **pupils in the home** e.g. DfE Umbrella scheme or LGfL HomeProtect filtering for the home and **remote-learning** procedures, rules and safeguards (see [remotesafe.lgfl.net](https://remotesafe.lgfl.net) for guidance to policies and an infographic overview of safeguarding considerations for remote teaching technology.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Network managers/technicians at LGfL schools may want to ensure that you take advantage of the following solutions which are part of your package: Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare. These solutions which are part of your package will help protect the network and users on it

### Marketing & Policy Officer – Alison Emmett

- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Executive Headteacher to ensure the school website meets statutory DfE requirements (see RAG-audit for \*MAINTAINED\*, \*FREE SCHOOL & ACADEMY\* websites at [safepolicies.lgfl.net](https://safepolicies.lgfl.net).)

### Data Protection Officer (DPO) – Maryline Avis

#### Key responsibilities:

- NB – this document is not for general data-protection guidance; GDPR information on the relationship between the school and LGfL can be found at [gdpr.lgfl.net](https://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 schools' (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 schools, 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](https://safepolicies.lgfl.net), but you should check the rules in your area.

- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above. You may be interested in the discounts for LGfL schools for three market-leading GDPR compliance solutions at [gdpr.lgfl.net](https://gdpr.lgfl.net)
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

## LGfL TRUSTnet Nominated contacts – **Helen Currie, Hasina Rashid, and Sean McLean (SSC)**

### Key responsibilities:

- To ensure all LGfL services are managed on behalf of the school in line with school policies, following data handling procedures as relevant
- Work closely with the DSL and DPO to ensure they understand who the nominated contacts are and what they can do / 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 and monitoring 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 school and LGfL at [gdpr.lgfl.net](https://gdpr.lgfl.net)
- SSC provides advice, can make changes to the security, filtering or firewall systems that are authorised by a recognised decision maker in the schools.

## Volunteers and contractors (including tutor)

### Key responsibilities:

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

## Children

### Key responsibilities:

- We only ever use technology (programmable toys, iPads, Cameras, school computers or whiteboards) with adult assistance. We do not have individual logins or user names and cannot access the internet without help.
- We talk about what we watch at home to make sure we are safe.
- Children can message their key person or teacher using Class Dojo with the help of their parents.
- We will tell an adult if we see something we don't like.
- We will only watch YouTube with our mums or dads.
- We will be gentle when using school technology.

## Parents/carers

### Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) **as part of the schools Admissions form** and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available in the [Online Tutors – Guidance for Parents and Carers](#) poster at [parentsafe.lgfl.net](https://parentsafe.lgfl.net), which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online

### External groups including parent associations – **Friends of FANS**

#### Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

### Education and curriculum

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

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE) **in accordance with the EYFS curriculum (Personal, Social and Emotional Development)**
- Computing **in accordance with Technology (Understanding the World)**
- Citizenship **in accordance with People and communities (Understanding the World)**

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

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

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

At **FANS** we recognise that online safety and broader digital resilience must be thread throughout the **EYFS** curriculum.

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 **Personal Social and Emotional Development, Technology and People and Communities, Understanding the World.**

## 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 support children **in line with our behaviour policy, Getting Along Together.**

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy, **which includes Sexual Harassment / Peer on Peer Abuse Policy**
- Anti-Bullying Policy **and** Behaviour Policy: **Getting Along Together**
- 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 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 pupils when they come into school or during extended periods away from school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

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

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

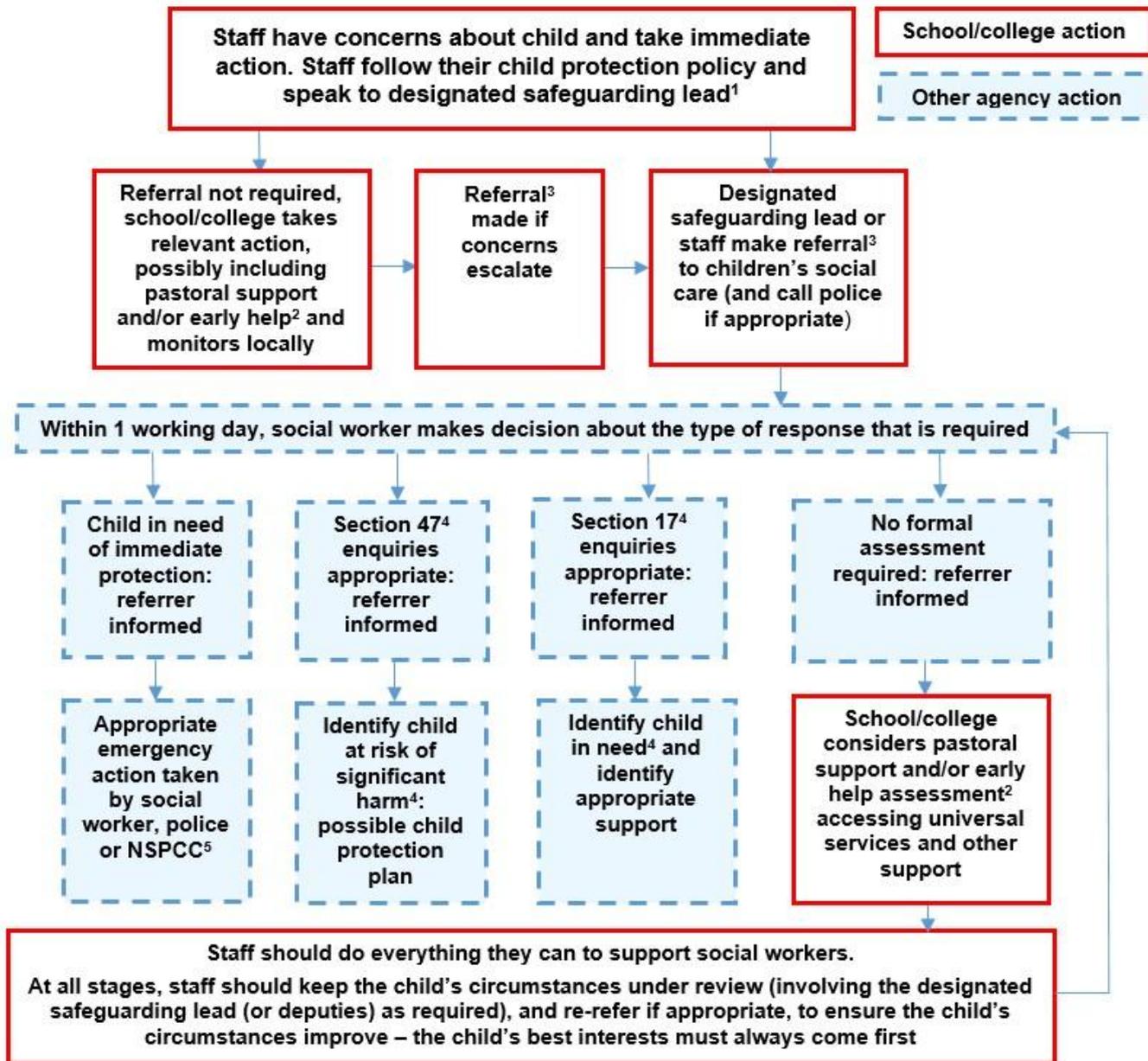
The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and 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).

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

### **Actions where there are concerns about a child**

The following flow chart (it cannot be edited) is taken from page 22 of Keeping Children Safe in Education 2021 as the key education safeguarding document. As outlined previously, online safety

concerns are no different to any other safeguarding concern.

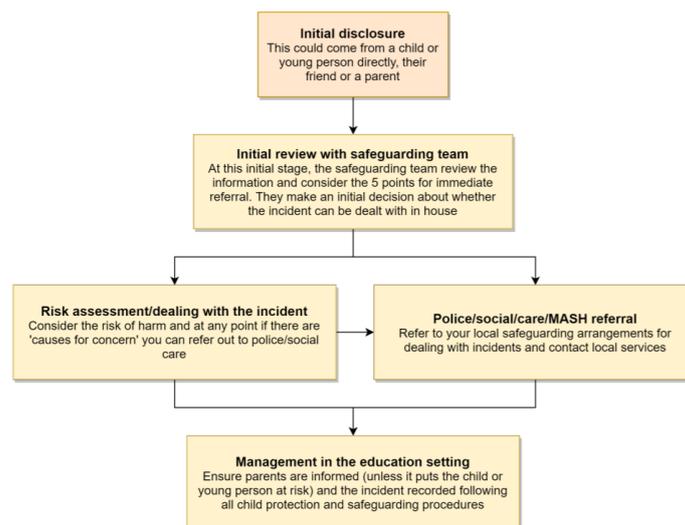


## Sexting – sharing nudes and semi-nudes

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

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

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



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

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

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

The documents referenced above and materials to support teaching about sexting can be found at [sexting.lgfl.net](http://sexting.lgfl.net)

## Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, 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 dealt with following the 'Dealing with signs of stress' section of **Getting Along Together**. Online bullying may also be referred to as cyberbullying, including issues arising from banter. **Getting Along Together** can be found here:

<H:\POLICIES & PROCEDURES\Child-focused policies\School Behaviour Policy>

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at [bullying.lgfl.net](http://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 45-49 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 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 pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). **Children at FANS can only use technology with adult guidance.**

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

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

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

## Social media incidents

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

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

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

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

## Data protection and data security

GDPR information on the relationship between the school and LGfL can be found at [gdpr.lgfl.net](https://gdpr.lgfl.net); there are useful links and documents to support schools with data protection in the 'Resources for Schools' 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' (August 2018), 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 schools, 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."**

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements, which can be found [here](#). Furthermore, this school makes use of the following discounted GDPR solution from LGfL:

- GDPR.co.uk from GRCI Law Ltd

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, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare.

The executive headteacher, data protection officer and governors 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 **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.

[ Schools may choose to reference some/all of the following topics here but in the light of GDPR they may be better exclusively in in your new data-protection documentation, or simply ensure that the policy for these areas is clear in data-protection documentation:

- CCTV: see CCTV Policy; only accessible by authorised staff; password protected
- Personal devices should not be used in the school, the school should provide school devices for the staff to use.
- Password policy / two-factor authentication: Nominated contacts in schools should be prompted to change their passwords every 90 days. LGFL, SIMS / FMS and other passwords are advised to be changed manually. We limit the number of times users can fail to log in before the system locks.
- Reminders to lock devices when leaving unattended

- Device encryption: we do not use device encryption unless the school has purchased encrypted USB memory sticks or encrypted USB hard drives.
- Access to and access audit logs for school systems
- Backups: backups for our sites key admin data, SIMS, FMS, admin staff home folders and Admin Shared areas are backed up to the LGFL cloud server (Gridstore). This is an encrypted backup system.
- Security processes and policies: SSC requires authorisation from a recognised person who is authorised to authenticate security and permission changes within the site.
- Disaster recovery: provided by SSC. They can in the event of a disaster, recover data from the cloud and reconfigure our new systems for use.
- Access by third parties, e.g. IT support agencies: Access by third parties is managed by SSC. The authorisation for a third party access will be authenticated by a recognised person with the site who is authorised to authenticate security and permission changes within the site. This is Hasina Rashid (Business Manager)
- BYOD: the wireless networks at the school are encrypted. The school devices are protected from outside infections by Sophos Anti-Virus. The school systems will allow devices to connect to the schools' broadband systems for internet access. The password for this access is protected by the school admin staff and provided only to users requesting this password / access once authorised. Further access to the server data, SIMS, FMS and stored documents is protected by the server permissions and is only accessible with a username and password for the required systems. The setup and configuration of the user account is managed by SSC and the Business Manager, Hasina Rashid who authorise all requests with a recognised person who is authorised to authenticate security and permission changes within the site.
- Wireless access: the wireless networks at the school are encrypted. The school systems will allow devices to connect to the schools' broadband systems for internet access. The password for this access is protected by the school admin staff and provided only to users requesting this password / access once authorised.
- File sharing: the school has access to various file sharing facilities. RAV3 remote access is a secure system for accessing files within the school and from home. LGFL email systems are internally encrypted (emails outside of the LGFL are not encrypted, Hotmail, Gmail etc). The LGFL also provide MyUSO cloud storage and file sharing, also a secure and encrypted system protected by usernames and passwords. Our nominated contacts can configure the permissions applied to this system.
- Cloud platform use, access and sharing protocols: Cloud Platform Use. Our site uses the LGFL HUB, the Waltham Forest HUB, the DFE secure data access sites, HSBC online budget planning software, LGFL Cloud Backup, LGFL MyUSO cloud storage/file sharing and LGFL email. All of these systems are encrypted and are secure sites, the exception being LGFL email which is encrypted LGFL to LGFL but not to external email systems – Hotmail, Gmail etc.

## Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools 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 school, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools. You can read more about why this system is appropriate on the UK Safer Internet Centre’s appropriate filtering submission pages [here](#).

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

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

At FANS we have decided that option 1 is appropriate for our work with 2 to 4 year olds that are unable to access the internet without adult support. All technology (toys, iPads, class computers and the interactive whiteboards) are only every used with an adult.

Children at FANS do not take this technology home.

Children are unable to log into any school system on a personal device.

We employ option 3 to cover adults’ use of technology.

## Electronic communications

Please read this section alongside references to pupil-staff communications in the overall school 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

- Staff at this school use the StaffMail system for all school emails

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

General principles for email use are as follows:

- Email and **Class Dojo** are 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 / executive 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/Executive Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately. **Families can also communicate with key people and class teachers using class Dojo.**
- Staff or pupil personal data should never be sent/shared/stored on email.
  - If data needs to be shared with external agencies, **use Egress Switch.**
  - Internally, staff should use the school network, including when working from home when remote access is available via the **RAV3 system or Freedom2Roam systems.**
- 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 are NOT allowed to 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 Executive Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to **Alison Emmett**. The site is managed by / hosted by [e4education](#)

The DfE has determined information which must be available on a school website. LGfL has compiled RAG (red-amber-green) audits at [safepolicies.lgfl.net](https://safepolicies.lgfl.net) to help schools to ensure that requirements are met (see appendices). **Note that an RSHE policy is now included.**

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

- Schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. If in doubt, check with **Hasina Rashid**. 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 schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net

- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

## Cloud platforms

It is important to consider data protection before adopting a cloud platform or service – see our DP policy [here](#).

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

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

## Digital images and video

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

- For photos/videos to be taken
- For the child's learning record
- For displays around the school and their name card
- For the school prospectus, on the school website, and on leaflets and posters advertising activities run by school

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 school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At **FANS** no member of staff will ever use their personal phone to capture photos or videos of pupils).

Photos are stored on the school network or on an external hard drive that is kept in a locked cabinet at **Church Hill** in line with the retention schedule of the school Data Protection Policy.

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

As we work with very young children we follow the EYFS curriculum in regard to programmable toys, using a simple computer program and choosing which technology is best to record images or videos. We do not cover KS1 curriculum for technology or computing.

## Social media

### **FANS' SM presence**

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

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online (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](mailto:helpline@saferinternet.org.uk)) involve schools' (and staff members') online reputation.

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

**Alison Emmett** is responsible for managing our Twitter/Facebook/Instagram social media accounts and checking our Wikipedia and Google reviews. They follow the guidance in the LGfL / Safer Internet Centre online-reputation management document [here](#).

### **Staff, pupils' and parents' SM presence**

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

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

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school [complaints procedure](#) should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+). 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 Online Harms regulation is likely to require more stringent age verification measures over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. **As our technology teaching centres around programmable toys, recording using technology and simple compute programs we do not teach about social media directly as we follow EYFS guidance, however,** children will often learn most from the models of behaviour they see and experience, which will often be from adults.

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

The school has official Church Hill, Low Hall and FANS Facebook / Twitter / Instagram accounts (managed by **Alison Emmett** and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children. **Families can email or use Class Dojo for these purposes.**

Email is the official electronic communication channel between parents and the school, and between staff and pupils. **Parents and practitioners can also use Class Dojo to communicate about their child's home learning. Parents can upload photos of their child onto their individual profile. This can then be shared with all families if we have permission from the child's parent. The content of Class Dojo is monitored by Helen Currie and Lindsay Read. Practitioners uploading videos of themselves send them to Lindsay or Helen first before they are uploaded.**

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

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

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

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

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

The serious consequences of inappropriate behaviour on social media are underlined by the fact that during the last 5 years, there have been 263 Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video (see page 28) and permission is sought before uploading photographs, videos or any other information about other people.

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

[\\10.243.114.20\Federation\\$\POLICIES & PROCEDURES\Safeguarding\e-safety policies\e-safety 2021-22](\\10.243.114.20\Federation$\POLICIES & PROCEDURES\Safeguarding\e-safety policies\e-safety 2021-22)

and the Data Protection Policy here:

<https://www.fans.waltham.sch.uk/quality-education/our-policies>

## Device usage

Remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with 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)

- **All staff who work directly with children** should leave their mobile phones switched off in one of the private staff areas during sessions and during school hours only use them in those private staff areas when they are on a break. See also the Digital images and video section on page 28 and Data protection and data security section on page 23. Child/staff data should never be downloaded onto a private phone. Voice recordings of children or staff is strictly prohibited except as part of our technology teaching. We do not record meetings at FANS. Doing so without permission could lead to disciplinary procedures. If we record the children as part of our technology teaching we will always talk to them about why and how we are recording and if they don't want to partake they don't have to. This is for learning purposes only and will not be added to public forums without parental permission first. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings),

permission of the executive headteacher should be sought (the executive 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 school events, please refer to the Digital images and video section of this document on page 28. [[parentfilming.lgfl.net](https://parentfilming.lgfl.net) may provide further useful guidance].

## Network / internet access on school devices

- **Pupils/students** are not allowed networked file access via personal devices.
- **Home devices** for vulnerable students / from the DfE scheme / LGfL Bridge the Divide programme / as part of a school 1-2-1 device scheme might be issued to some students in case of a future lockdown. These are restricted to the apps/software installed by the school and may be used for learning and reasonable and appropriate personal use at home, but all usage may be tracked. The devices would be fitted with the LGfL HomeProtect home filtering.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section on page 28 and Data protection and data security section on page 23. Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** have no access to the school network or wireless internet on personal devices. All internet traffic is monitored.
- **Parents** have no access to the school network or wireless internet on personal. All internet traffic is monitored.

## Trips / events away from school

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

## Searching and confiscation

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

## Appendices

Guidance for LGfL schools about how we work with your data can be found [here](#); helpful resources for all schools can be found [here](#) ]

Where marked with \* the latest version or a template you may use is available at [safepolicies.lgfl.net](https://safepolicies.lgfl.net)

1. Safeguarding Incident log
2. [Safeguarding and Child Protection Policy](#)
3. [Behaviour Policy / Anti-Bullying Policy 'Getting Along Together'](#)
4. [Staff Code of Conduct](#)
5. \*[Acceptable Use Policies](#) (AUPs) for:
  - \*Pupils
  - \*Staff, Volunteers Governors & Contractors
  - \*Parents
6. \*Letter to parents about filming/photographing/streaming school events
7. \*Prevent Risk Assessment Template
8. \*[Online-Safety Questions from the Governing Board](#) (UKCIS)
9. \*[Education for a Connected World cross-curricular digital resilience framework](#) (UKCIS)
10. \*[Safer working practice for those working with children & young people in education](#) (Safer Recruitment Consortium); their [April 2020 Addendum](#)
11. \*[Working together to safeguard children](#) (DfE)
12. \*[Searching, screening and confiscation advice](#) (DfE)
13. \*[Sexual violence and sexual harassment between children in schools and colleges](#) (DfE advice)
14. \*Sharing nudes and semi-nudes guidance from UKCIS:
  - \*[How to respond to an incident - overview for all staff](#)
  - \*[Full guidance for school DSLs](#)
  - \*[Online Safety Audit for Trainee \(ITT\) & Newly Qualified Teachers \(NQT\)](#)
15. \*[Prevent Duty Guidance for Schools](#) (DfE and Home Office documents)
16. [Data protection and data security advice, procedures etc](#)
17. \*[Preventing and tackling bullying](#) (DfE)
18. Cyber bullying: advice for headteachers and school staff (DfE) – find this at [bullying.lgfl.net](https://bullying.lgfl.net)
19. \*[RAG \(red-amber-green\) audits for statutory requirements of school websites](#)
20. \*[Ofsted Review of sexual abuse in schools and colleges](#)

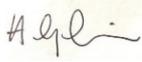
---

The Premises Committee of the Governing Body approved this policy:





Name: Pauline France .....



Name: Helen Currie.....

Date: 16/11/21 .....