

St John Fisher RC Primary School

Online Safety Policy



LOVE LEARN ACHIEVE

St John Fisher Mission Statement

The school, in partnership with parents, carers and with the parish of St John Fisher, offers to each one of its children a Catholic education centred on Christ, which enables them to grow in God's love, learning to be the best they can be in accordance with Christian values.

Approved by:

Mrs. K. Blom

Date: January 2023

Last reviewed on:

January 2023

Next review due by:

January 2024

	St John Fisher RC Primary School	
	Policy review Date	January 2023
	Date of next Review	January 2024
	Designated Safeguarding Lead (DSL) team	Janine Kenna Claire Ellerker Claire Higgins

This policy is part of the School's Statutory Safeguarding Policy. It applies to all members of the school (including staff, governors, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Contents

1. Introduction and Overview
 - Rationale and Scope
 - Roles and responsibilities
 - How the policy is communicated to staff/pupils/community
 - Handling Incidents
 - Reviewing and Monitoring
2. Education and Curriculum
3. Handling online safety concerns and incidents
4. Managing the IT Infrastructure
 - Internet access, security (virus protection) and filtering
 - Network management (user access, backup, curriculum and admin)
 - Passwords
 - E-mail
 - School website
 - Learning platforms (Cloud environments)
 - Social media
 - CCTV
5. Data Protection and Data Security
6. Equipment and Digital Content
 - Personal mobile phones and devices
 - Digital images and video

Appendices:

Appendix 1 - Roles and responsibilities

All staff

Headteacher

Designated Safeguarding Leads

Governing Body

Network Manager

Data Protection Officer

Volunteers and Contractors

Pupils

Appendix 2

Acceptable Use Agreement (Staff, Volunteers and Governors)

Acceptable Use Agreements (Pupils – adapted for phase)

Acceptable Use Agreement including photo/video permission (Parents)

NB: These can be found as separate documents in the Policies section of school website

A1: GDPR: General Data Protection Regulations [link](#)

1. Introduction and Overview

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach. Accordingly, this policy is written in line with ‘Keeping Children Safe in Education’ 2022 (KCSIE), ‘Teaching Online Safety in Schools’ 2019, statutory RSHE guidance 2019 and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside our school’s statutory Safeguarding Policy. Any issues and concerns with online safety must always follow the school’s safeguarding and child protection procedures.

Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct or Commerce (see section 135 of KCSIE 2022). These areas provide a helpful approach to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, and it is important to understand the interplay between all of these. This is evident in Ofcom’s Media and Attitudes Report 2022 which suggests 36% of children aged 8-17 had seen something ‘worrying or nasty’ online in the past 12 months, with 84% experiencing bullying via text or messaging, on social media, in online games, through phone or video calls, or via other apps and sites.

Analysis from the Centre of Expertise on Child Sexual Abuse also highlights the prevalence of child sexual abuse, with 500,000 children estimated to experience child sexual abuse every year, whilst the Internet Watch Foundation has identified the growing risk of children, with a three-fold increase in abuse imagery of 7–10-year-olds. This highlights transition years as crucial in the fight against sexual exploitation, in primary and secondary.

Following Covid-19 it is important to remember that more time spent online increases the risk for grooming and exploitation (CSE, CCE and radicalisation) and potentially reduces opportunities to disclose such abuse. Teachers may also find LGfL’s SafeSkills Online Safety Quiz and diagnostic teaching tool at safeskillsinfo.lgfl.net particularly useful to capture and assess pupil resilience and competence for digital life, as recommended by KCSIE.

Rationale

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all St John Fisher RC Primary community members’ online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Safeguard and protect the children and staff.

- Helping safeguarding and senior leadership teams to have a better understanding and awareness of filtering and monitoring through effective collaboration and communication with technical colleagues.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating 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.
- Helping 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,
 - 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
- Establishing 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 Relationships & Behaviour Policy or Anti-Bullying Policy)

Scope

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

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

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.

Depending on their role, all members of the school community should read the relevant section in Annex A of this document that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also role descriptions in the annex.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and staff website.
- Policy to be part of the school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable Use Agreements discussed with staff and pupils at the start of each year and parents redirected to them at the start of an academic year. Acceptable use agreements to be issued to the whole school community, on entry to the school.

Handling Incidents

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Designated Safeguarding Lead acts as the first point of contact for any incident.
- Any suspected online risk or infringement is reported to a Designated Safeguarding Lead that day.
- Any concern 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).
- See further details below under 'Handling online safety concerns and incidents'.

Reviewing and Monitoring Online Safety

The Online Safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Social Media).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school Online Safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

At St John Fisher RC Primary School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum.

This school:

- Has a clear, progressive online safety education programme as part of the PSHE and Computing curriculum and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience, building on what pupils have already learned and identifying subject content that is appropriate for their stage of development.
- Encourages staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum leads, and making the most of unexpected learning opportunities as they arise (which

have a unique value for pupils). In order to support them with this, all teachers have access to [Project Evolve](#) (SWGfL), providing them with resources for each of the 330 statements from UK Council for Internet Safety's (UKCIS) framework "Education for a Connected World".

- Reminds pupils about their responsibilities through the pupil Acceptable Use Agreement(s);
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- Ensure all staff comply with GDPR (General Data Protection Regulation)
- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.
- Ensures staff encourage sensible use whenever overseeing the use of technology, monitoring what pupils are doing and consider potential dangers and the age appropriateness of websites (even with filtering and monitoring policies in place).
- Ensures staff support pupils with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

"Parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online." (KCSIE 2022)

Staff and governor training

This school:

- Makes regular training available to staff on online safety issues and the school's online safety education program;
- Provides, as part of the induction process, all new staff with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness

This school:

- Provides information for parents which includes online safety;
- Provides parents with information about online safety and how they can inform the school/report incidents to the school.

3. 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 PSHE/RSHE and Citizenship, and Computing).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side

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

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence). School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Sexual Harassment / Peer on Peer Abuse Policy (if separate)
- Anti-Bullying Policy / Social Media Policy
- Relationships and Behaviour Policy (including school consequences)
- 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 designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

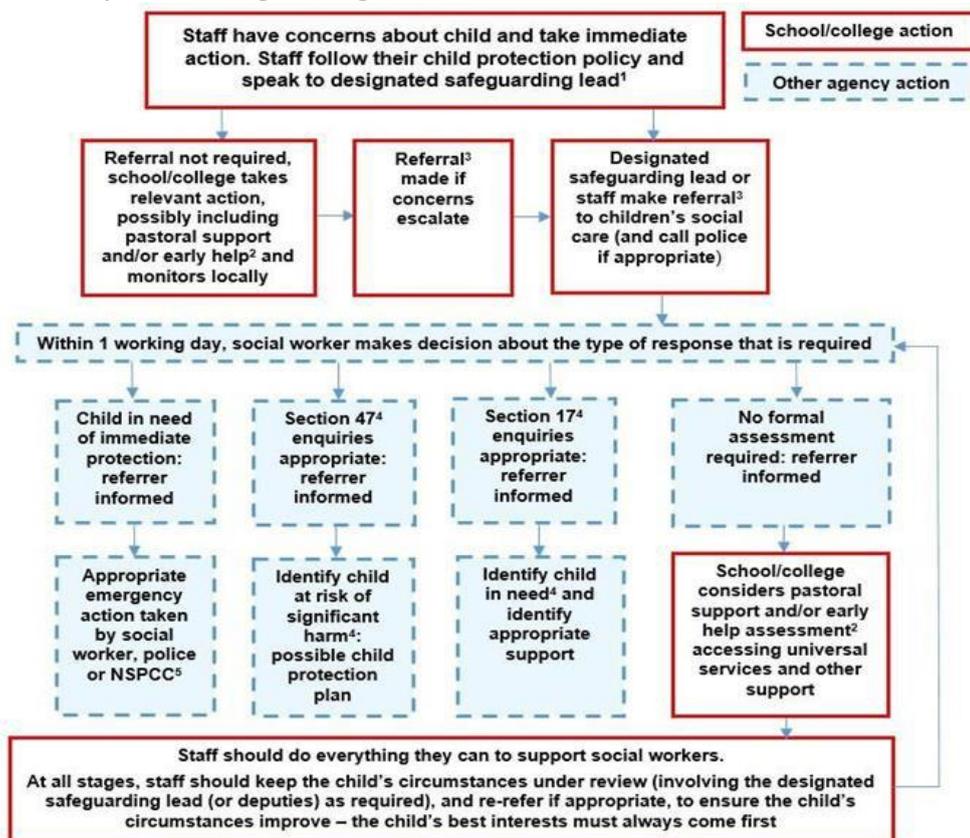
The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The new DfE guidance [Behaviour in Schools, advice for head teachers and school staff](#) July 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 32-34 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

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 and make alternative provisions in advance where these might be needed.

Actions where there are concerns about a child

The following flow chart is taken from page 22 of Keeping Children Safe in Education 2022 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

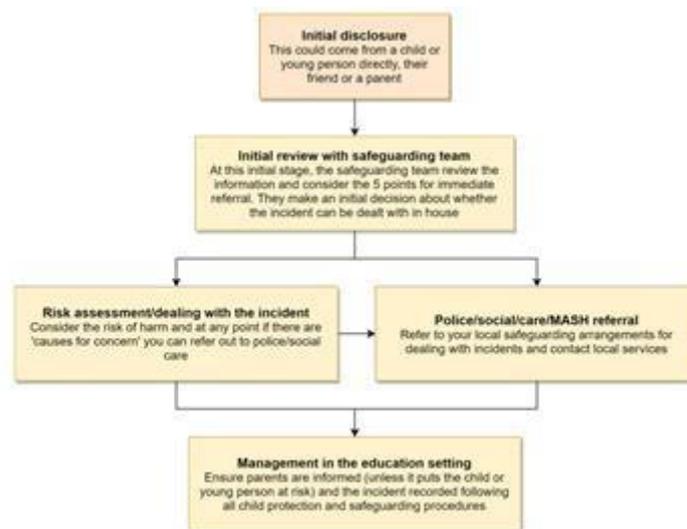


Sexting – sharing nudes and semi-nudes

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) 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 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, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child on child abuse pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

Online Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter. 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 has now been incorporated into Keeping Children Safe in Education and is no longer a document in its own right. It would be useful for all staff to be aware of this updated guidance: Part 5 covers the immediate response to a

report, providing reassurance 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 and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. 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).

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/clouds, devices and other technology.

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

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 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 within this document for rules and expectations of behaviour for children and adults in the St John Fisher RC Primary 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, the school will request that the post be deleted and will expect this to be actioned promptly.

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

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

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.

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

This school:

- informs all users that both Internet and email use is monitored;
- has the educational filtered secure broadband connectivity through the LGfL;
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved ‘web filtering management’ status;
- uses USO user-level filtering where relevant;
- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2 to send ‘protect-level’ (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access ‘protect-level’ (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect pupils.
- Ensures visitors and guests are provided with information on a guest log in and guest Wi-Fi access as appropriate.
- At home, all devices are the responsibility of the parent to ensure online safety. School devices in the home, do not have any additional school controls when not on the school site.
- When pupils access their school GSuite account on a personal device, the GSuite filtering extension will be applied when logging into a home Chromebook and also when logging into a Chrome profile on a Windows laptop.

Network management (user access, backup)

This school:

- Uses individual, audited log-ins for all users - the LGfL USO system;
- Has additional local network monitoring/auditing software installed;
- Ensures the Systems IT provider is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the [EU data protection directive](#) where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff have read and understand the school's Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Requires all users to log off/lock their device when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
e.g. Borough email or Intranet; finance system, Personnel system etc.
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote offsite back up of data;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent via USO secure file exchange (USO FX).
- Ensures that school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are to be encrypted.
- Requires any loss or theft of device, such as laptop or USB drive, to be brought to the attention of the head teacher immediately. The head teacher will liaise with the online safety governor to ascertain whether a report needs to be made to the Information Commissioner's Office.
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Passwords

- This school makes it clear that staff and pupils must always keep their passwords private and must not share them with others. If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff using critical systems to use two factor authentication.
- All staff print all documents securely through the password pin retrieval.

Email

This school:

- Provides staff with an LGfL email account for their professional use (London Staffmail) and makes clear personal email should be through a separate account;
- We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk/head@schoolname.la.sch.uk
- Will contact the Police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

- Pupils do not have access to emails at school.
- Pupils are taught about the online safety of using e-mail in school and parents are encouraged to continue this online safety support at home.

Staff:

- Staff use LGfL email systems and Gmail on the school system.
- Staff will use LGfL email systems for professional purposes.
- These systems are 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.
- Access in school to external personal email accounts may be blocked.
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.
- Google Classroom/Google Drive is the only means of electronic communication to be used between staff and pupils.
- LGfL Email is the only means of electronic communication to be used between staff and parents.
- Use of a different platform must be approved in advance by the headteacher. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (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. Internally, staff should use the Google Drive school network, including when working from home when remote access is available via the RAV3 system.

School website

- The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The

Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to the Deputy Headteacher. The site is managed by / hosted by FSE Design.

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Where other staff submit information for the website, they are asked to remember that sources must always be credited and material only used with permission.
- The school website complies with statutory DFE and GDPR requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Cloud Environments - Google Classroom

- Pupils use GSuite for Education both in school and for home learning - these are a set of education tools from Google including Google Classroom and Google Drive. Pupils use their GSuite accounts to complete homework assignments.
- Pupils access their GSuite account using their own individual Gmail login and password GSuite for Education. Documents pupils upload onto Google Drive cannot be shared with external email accounts, only with others within @gsuite.st-johnfisher.merton.sch.uk - the school's Google domain.
- Uploading of information onto Google Classroom is shared between different staff members according to their responsibilities e.g. class teachers upload weekly homework to their year group's Google Classroom.
- Google Cloud contains much of the electronic work that pupils complete in school. By logging in at home, using the same login as at school, pupils may continue working on projects started in school, often using one of the main apps of GSuite, Google Classroom. Google's Privacy Policy for GSuite can be found here:
<https://policies.google.com/privacy/update>
- In school, pupils are only able to upload and publish work within school approved 'Cloud' systems (i.e. GSuite).
- Google Classroom/Google Drive is the only means of electronic communication to be used between staff and pupils.

Social Media

This section should be read in conjunction with the school's Social Media policy (available in the *policies' section of the school website*)

St John Fisher manage and monitor their 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.

Social media (including 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 [[Complaints Policy](#)] 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+), but the school regularly deals with issues arising on social media with pupils/pupils 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 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 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, 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).

The school has an official Twitter account (managed by the Deputy Headteacher). However, email is the official electronic communication channel between parents and the school.

Pupils 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.

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

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

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

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

CCTV

- We have CCTV in the school as part of our site surveillance for staff and pupil safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5. Data Protection and Data Security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements, which can be found here. [[Data Protection Policy](#)]

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: these products are all available from LGfL, USO sign on for LGfL services, Sophos Anti-Virus, Sophos InterceptX, Sophos Server Advance.

The 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 USO-FX 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.

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear on who the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out or lock systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to [The Waste Electrical and Electronic Equipment Regulations 2006](#) and/or [The Waste Electrical and Electronic Equipment \(Amendment\) Regulations 2007](#). [Further information](#) can be found on the Environment Agency website.

- Disposal of any equipment will conform to the Data Protection Act 1998 and the advice of the Information Commissioner's Office
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

6. Equipment and Digital Content

- Mobile devices (Mobile phones, tablets and other mobile devices) brought into school are entirely at the staff member, pupils, parents or visitors' own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- No pupils should bring his or her mobile phone or personally-owned device into school unless this is authorised by a parent/carer. Any pupil device brought into school will be safely stored in the office or locked in the classroom cupboard (for Year 6 pupils). All devices will be signed in and signed out.
- Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher/SLT.
- Mobile devices will not be used for personal reasons in any way during lessons or formal school time. They should be switched off or silent at all times.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned and approved by Headteacher/SLT.
- Staff members may use their phones during school break times away from children.
- All visitors are requested to keep their phones on silent, in private areas out of sight from children.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher and a Personal Device agreement has been signed. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The school reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobile devices may be searched at any time as part of routine monitoring.

School Owned Devices

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Personal Devices

Pupils' use of personal devices

- The school strongly advises that pupil mobile phones and devices should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a pupil breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff are encouraged not to use their own mobile phones or devices in a professional capacity. Where mobile phones must be used (for example to contact a parent during a parent consultation when working from home) teachers must withhold their number by adjusting the settings on their mobile device.
- Staff will be issued with a school phone where contact with pupils, parents or carers is required, for instance for off-site activities.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the SLT.
- If a member of staff breaches the school policy then disciplinary action may be taken

Trips and 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 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 pupil 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 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.

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually).;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials;
- 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 St John Fisher, members of staff may occasionally use personal devices to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.
- For long term, high profile use of specific pupil photos (not group photos) on the school website, in the prospectus or in other high profile publications the school may seek to obtain individual parental or pupil permission;
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. 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 are subject to bullying or abuse.
- Staff 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.

Appendix 1 – Roles and responsibilities

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

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

Roles:

- All Staff
- Headteacher
- Governing Body, led by Safeguarding Link Governor
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Pupils
- Parents/carers
- External groups including parent associations

Role	Key Responsibilities
<p>All staff</p>	<ul style="list-style-type: none"> ● Read and follow this policy in conjunction with the school’s main safeguarding policy and the relevant parts of Keeping Children Safe in Education ● Understand that online safety is a core part of safeguarding and part of everyone’s job – never think that someone else will pick it up. Safeguarding is often referred to as a jigsaw puzzle – you may have the missing piece, so do not keep anything to yourself. Record online-safety incidents in the same way as any safeguarding incident; report in accordance with school procedures ● Know who the Designated Safeguarding Lead (DSL) is; notify them not just of concerns but also of trends and general issues you may identify. Also speak to them if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon ● Sign and follow the staff acceptable use policy and code of conduct ● Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE and Computing curriculum, both outside the classroom and within the curriculum, supporting curriculum/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 and how they keep children safe).

	<ul style="list-style-type: none"> ● Follow best-practice pedagogy for online-safety education, avoiding scaring, victim-blaming language and other unhelpful prevention methods. ● When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the 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 protection and phishing strategies. ● Prepare and check all online sources and classroom resources before using for accuracy and appropriateness. ● Encourage pupils to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions. ● Take a zero-tolerance approach to all forms of child-on-child abuse - this includes bullying, sexual violence and harassment. ● Be aware that you are often most likely to see or overhear online-safety issues in the playground, corridors and other communal areas outside the classroom – let the DSL know. ● Receive regular updates from the DSL and have a healthy curiosity for online safeguarding issues ● Model safe, responsible and professional behaviours in your own use of technology This includes outside 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.
<p>Headteacher</p>	<ul style="list-style-type: none"> ● Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding ● Oversee and support the activities of the designated safeguarding lead team and ensure they work with colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school) ● Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance ● Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures

	<ul style="list-style-type: none"> ● Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school’s arrangements. ● Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles ● Liaise with technical colleagues on a regular basis to have an understanding and awareness of filtering and monitoring provisions and manage them effectively – in particular understand what is blocked or allowed for whom, when, and how. Note that KCSIE 2022 strengthens the wording for this. ● 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 ● Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards ● Assign responsibility to a nominated member of staff (School Business Manager) to carry out online searches with consistent guidelines as part of due diligence for the recruitment shortlist process. ● 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 ● Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident ● Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised ● Ensure the school website meets statutory requirements
<p>Designated Safeguarding Lead</p>	<ul style="list-style-type: none"> ● “The designated safeguarding lead should take lead responsibility for safeguarding and child protection [including online safety] ... this lead responsibility should not be delegated”. ● Ensure “An effective whole school 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.” ● Ensure ALL staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated.

- Liaise with the Headteacher and Chair of Governors to ensure that ALL governors and trustees undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated.
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious 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 SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school).
- 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 and 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 for examples or sign up to the [LGfL safeguarding newsletter](https://www.lgfl.gov.uk/safeguarding-newsletter)
- 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.ukcisa.org.uk/education-for-a-connected-world-2020-edition)’) and beyond, in wider school life
- Promote an awareness of and commitment to online safety throughout the school community
- 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.
- Oversee and discuss ‘appropriate filtering and monitoring’ with governors and ensure staff are also aware. Liaise with technical teams and ensure they are implementing not taking the strategic decisions on what is allowed and blocked

	<p>and why. Also, as per KCSIE “be careful that ‘over blocking’ does not lead to unreasonable restrictions”.</p> <ul style="list-style-type: none"> ● Ensure KCSIE ‘Part 5: Sexual Violence & Sexual Harassment’ is understood and followed throughout the school and that staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don’t dismiss it as banter (including bullying). ● Facilitate training and advice for all staff, including supply teachers: <ul style="list-style-type: none"> - all staff must read KCSIE Part 1 and all those working with children
<p>Governing Body, led by Safeguarding Link Governor</p>	<ul style="list-style-type: none"> ● Approve this policy and strategy and subsequently review its effectiveness ● Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated ● Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated ● 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. ● Support the school in encouraging parents and the wider community to become engaged in online safety activities ● Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at governor meetings ● Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information ● Ensure that children are taught about safeguarding, including online safety, as part of providing a broad and balanced curriculum
<p>PHSE/RSHE Lead</p>	<p>As listed in the ‘all staff’ section, plus:</p> <ul style="list-style-type: none"> ● 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. ● Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app. ● Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE. ● Note that an RSHE policy should be included on the school website. ● Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach
<p>Computing Lead</p>	<ul style="list-style-type: none"> ● As listed in the ‘all staff’ section, plus:

	<ul style="list-style-type: none"> ● Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum ● Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach ● Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing ● Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements
Class teachers	<ul style="list-style-type: none"> ● Embed online safety in the curriculum ● Supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) ● Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws. ● Ensure all digital communication with pupils and parents/carers is professional and only carried out using official school systems. ● Ensure that - in lessons where internet use is planned - pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. ● Ensure that any online safety incident is reported to a DSL and recorded.
Network Manager/technician	<ul style="list-style-type: none"> ● As listed in the 'all staff' section, plus: ● Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology. Note that KCSIE changes expect a great understanding of technology and its role in safeguarding, so help DSLs and SLT to understand systems, settings and implications. ● Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE), protections for pupils in the home and remote-learning. ● Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant ● Work closely with the designated safeguarding lead/ data protection officer to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice. ● 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. ● 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.

	<ul style="list-style-type: none"> ● Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy. ● Work with the Headteacher to ensure the school website meets statutory DfE requirements.
Data Protection Officer	<ul style="list-style-type: none"> ● 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; 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 <u>all</u> 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 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 ● Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited
LGfL Nominated contact(s)	<ul style="list-style-type: none"> ● To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant.
Volunteers and contractors	<ul style="list-style-type: none"> ● Read, understand, sign and adhere to an acceptable use policy (AUP) ● Report any concerns, no matter how small, to the designated safety lead ● 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

	<ul style="list-style-type: none"> 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. <p>Exit strategy</p> <ul style="list-style-type: none"> At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include removal from management information system and networks that allow access to school based data, utilising information from school to secure exit procedures are carried out for leavers.
Pupils	<ul style="list-style-type: none"> Read, understand, sign and adhere to the pupil acceptable use policy and review this annually Treat home learning during any isolation or school lockdown in the same way as regular learning in school and behave as if a teacher or parent were watching the screen Avoid any private communication or use of personal logins/systems to communicate with school staff Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else. To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school’s acceptable use policies cover actions out of school, including on social media Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher. Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems To be critically aware of the materials/content they access online and be guided to consider the accuracy of information. To acknowledge the source of information used and to respect copyright when using material accessed on the internet
Parents/carers	<ul style="list-style-type: none"> Read, sign and promote the school’s parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it. Talk to 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, whether for homework or during any school closures or isolation and flag any concerns.

	<ul style="list-style-type: none"> ● In the case of remote learning (e.g. in quarantine), support the child during any home 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, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online.
<p>External groups including Parent groups</p>	<ul style="list-style-type: none"> ● Any external individual/organisation will read and understand the Acceptable Use Policy agreement prior to using technology or the Internet within school. ● To support the school in promoting online safety. ● To model safe, responsible and positive behaviours in their own use of technology.

Appendix 2 – Related Policies and Documents See [school website](#) for policies

1. Safeguarding and Child Protection Policy
2. Relationships and Behaviour Policy / Anti-Bullying Policy
3. Staff Code of Conduct / Handbook
4. Acceptable Use Policies (AUPs) for:
 - Pupils
 - Staff
5. Data protection policy