

What's different about this policy for September 2020 and during Covid-19?

The principles remain the same so this AUP is virtually unchanged this year. Nonetheless, we recommend you review all policies and AUPs in the light of school changes, closures, new remote technologies and an increase in online tutoring which may require reminders to all stakeholders about tutors' behaviour.

At <u>coronavirus.lgfl.net/safeguarding</u> you will find a document to help you review policies, guidance on the safe use of remote technology settings to look out for.

Cover sheet – delete this page once you have finished editing the document

- Whilst this document has been created in response to requests from schools for a standalone document, it is an extract from the LGfL DigiSafe main online safety policy template for schools, available at <u>safepolicies.lgfl.net</u>, with only minor alterations to make it work as a standalone document. If it is helpful in your context, you may decide to use it as a separate document, but you could also keep it within the main OS policy and simply refer to it wherever necessary (e.g. in Acceptable Use Policies; our templates allow you to do this).
- Please be careful that the messages here do not contradict others in your online safety or safeguarding policy, or acceptable use policies.
- Every school is different some will be more or less comfortable with the use of social media. However, even if you do not have school accounts or allow any use of social media in school or relating to school, it is important to nonetheless have a clear policy to avoid confusion. Equally, the principle applies that "If you aren't managing your social media presence, somebody else will".
- Before editing this document, please read the advice on the LGfL / UK SIC document on 'Managing your online reputation' at <u>onlinerep.lgfl.net</u>. Page 4 on your 'Online Media Strategy' is important to consider first.
- You will want to edit / remove / add items based on the knowledge of your school and your approach; it is impossible to give all options here.
- Items highlighted in yellow need editing/completing/removing before you issue the document
- Feel free to add your school name and logo, but please do not try to remove our branding/links
- We would love to hear how you use this policy / if it's useful, how we can improve it and what else we can do to support you get in touch with @LGfLDigiSafe on Facebook or Twitter
- Find our other templates for a School Online Safety Policy and Acceptable Use Policies for all members of the school community at <u>safepolicies.lgfl.net</u>.
- We also provide online safety educational resources (filtered by audience, theme or key stage) at <u>saferesources.lgfl.net</u>, and a range of materials to support outreach work with parents at <u>parentsafe.lgfl.net</u>



Social media 's SM presence

St. Saviour's 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: <u>helpline@saferinternet.org.uk</u>) 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.

Mr John Ward is responsible for managing our Twitter/Facebook/Website accounts and checking our Wikipedia and Google reviews. He follows the guidance in the LGfL / Safer Internet Centre online-reputation management document <u>here</u>.

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 which is on our website, 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 St Saviour's school regularly deals with issues arising on social media with 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/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

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

The school has a Twitter account (managed by Mr Ward) and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

Email, calling the office and speaking to an adult is the official electronic communication channel between parents and the school, and between staff and pupils.

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.

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

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/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 of the 131 Prohibition Orders issued to staff in 2017, 73 involved social media/technology (and 27 of the 66 orders by August 2018).

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 as requested from the School Business Manager.

Social media incidents

Breaches of this policy and of school AUPs (Acceptable Use Policies) will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, St Saviour's 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 where it is hosted, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process. The police or other authorities may be involved where a post is potentially illegal or dangerous.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature by the school. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Further questions

If parents have further questions, they can contact a member of the Senior Leadership Team, the Deputy or the School Business Manager at the school; the NSPCC has a parent online safety helpline which can help with general issues that are not school specific.

Staff should speak to the Deputy in the first instance, who may then call on the expertise of local authority and Diocesan advisers, LGfL DigiSafe or Professionals' Online-Safety Helpline (from UK SIC).