The principles remain the same in the present situation. However, key areas surround **home learning**, including **remote teaching technologies**, prevention of harm with more **time unsupervised and online at home**, as well as the use of **tutors** and checking all safeguarding measures are understood and applied by **supply teachers** (as per changes to KCSIE 2020). KCSIE 2020 also now mentions keeping children safe “including when they are **online at home**”.



|  |  |  |
| --- | --- | --- |
| **Approved by:** |  Governors  | **Date:**  |
| **Last reviewed on:** | Jan 2021 |
| **Next review due by:** | Jan 2023 |
|  |  |

# Introduction

## Key people

|  |  |  |
| --- | --- | --- |
| **St Margaret’s CE VA Primary School** | Designated Safeguarding Lead (DSL) team | Mrs Jayne StackhouseDeputy DSL Mr Stuart JonesCover DSL Mrs Ruth BoudMrs Celine HumphriesMrs Rachel Boyce  |
| Online Safety LeadOSL | Miss E O’Neill  |
| Online-safety / safeguardinglink governor | Rev M RutterMrs Denise Large  |
| PSHE/RSHE lead | Mrs C Humphries |
| Network manager/ technical support  | SIPS IT  |
| Data Protection Officer DPOWorking alongside Sandwell LAFor GDPR | Mrs J Stackhouse |
| Date this policy was reviewed and by whom | January 2021 |
| Date of next review and by whom | January 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’ 2020 (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 St Margaret’s school’s statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school’s safeguarding and child protection procedures.

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

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Any changes to this policy should be immediately disseminated to all the above stakeholders.

## Who is in charge of online safety?

The KCSIE makes it clear the designated safeguarding lead is responsible 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 2020, 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.

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 first lockdown. Pupil questionnaires can help inform any risks that may have occurred.

## How will this policy be communicated?

##

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 (AUP’s) 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

Aims

This policy aims to:

* Set out expectations for all St Margaret’s CE VA Primary community members’ online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
* Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
* Facilitate the safe, responsible and respectful use of technology to support teaching and 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 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, 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).

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 NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

## Scope

This policy applies to all members of the St Margaret’s CE VA Primary community (including)teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, governors, volunteers, contractors, pupils, parents/carers, and visitors 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

**Key responsibilities:**

* Work with SLT to review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
* Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
* 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 Deputy DSL and SLT on all Online Safety issues 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, Deputy 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 governors are regularly updated on the nature and effectiveness of the school’s arrangements for online safety
* Ensure the school website meets statutory requirements

## Designated Safeguarding Lead and Deputy Safeguarding Lead/ Online Safety Lead

**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 2020):

* “The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] … this **lead** responsibility should not be delegated”
* Work as a team with technical staff to review protections for **pupils in the home** and **remote-learning** procedures and rules.
* DSL ensure there is regular review and open communication between the Online Safety Lead
* Ensure there is “An effective approach to online safety [that] empowers school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.”
* “Liaise with staff (including support staff, IT Technicians, and SENCO) 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 fully 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 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.” Work with Sandwell Prevent Officer– see [safetraining.lgfl.net](https://www.lgfl.net/training/default.aspx?c=dac7c0c1-07ef-46f9-98a7-f6d6a8c3d62b) 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).
* Receive regular updates in online safety issues and legislation, be aware of local and school trends – see regular updates from local Sandwell Prevent Officer other examples include [safeblog.lgfl.net](https://safeblog.lgfl.net) , [LGfL safeguarding newsletter](https://safenewsletter.lgfl.net)
* Ensure that online safety education is regularly taught and 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’) and beyond, in wider school life
* Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, – materials at [parentsafe.lgfl.net](https://parentsafe.lgfl.net)
* Communicate regularly with SLT and the designated safeguarding and online safety governor to discuss current issues (anonymised), review incident logs and filtering. Ensure staff are aware of the filtering systems
* 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. Ensure pupils know how to report concerns.
* Ensure the 2018 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
* Facilitate training and advice for all staff, including supply teachers:
	+ all staff must read KCSIE Part 1 and all those working with children Annex A
	+ it would also be advisable for all staff to be aware of Annex C (online safety)
	+ cascade knowledge of risks and opportunities throughout the organisation
	+ [cpd.lgfl.net](http://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.

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

**Key responsibilities (quotes are taken from Keeping Children Safe in Education 2020)**

* 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](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/562876/Guidance_for_School_Governors_-_Question_list.pdf)
* Ask about how the school has reviewedprotections for **pupils in the home** and **remote-learning** procedures and rules.
* “Ensure an appropriate **senior member**, 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 and training.
* Have regular strategic reviews with the Online-Safety Lead / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
* DSL or deputy DSL, regularly meet with Online Safety Lead.
* Ensure there is 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 A; check that Annex C on Online Safety reflects practice in your school
* “Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction.
* “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”.
* “Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school approach to online safety with a clear policy on the use of mobile technology.”

## All staff

**Key responsibilities:**

* In 2021 pay particular attention to safeguarding provisions for **home-learning** and **remote-teaching**
* Recognise that **RSHE** will be introduced in this academic year and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
* 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)
* Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
* Read and follow this policy in conjunction with the 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
* 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, 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
* When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the [**20 Safeguarding Principles for Remote Lessons**](https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf) 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 suitable passwords and phishing strategies.
* Prepare and check all online sources and resources before using
* Encourage pupils 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.
* Take a zero-tolerance approach to bullying and low-level sexual harassment.
* 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](http://onlinerep.lgfl.net) guidance for schools.

## PSHE / RSHE Lead

**Key responsibilities:**

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

## Computing Lead –

**Key responsibilities:**

* As listed in the ‘all staff’ section, plus:
* Oversee the delivery of the online safety element of the Computing Curriculum in accordance with the national curriculum
* Work closely with the 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 to ensure a common and consistent approach, in line with acceptable-use agreements

## Subject 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

## Network Manager/technician SIPS

**Key responsibilities:**

* As listed in the ‘all staff’ section, plus:
* Support the HT and DSL team as they reviewprotections for **pupils in the home** and **remote-learning** procedures and rules.
* 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
* 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
* Monitor the use of school technology that any misuse/attempted misuse is identified and reported to the Headteacher

## Data Protection Officer (DPO) –

**Key responsibilities:**

* Be aware that of references to the relationship betweendata 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.”
* Work with the Deputy DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
* Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

## Volunteers and contractors (including Tutors)

**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 leader
* 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.

## Pupils

**Key responsibilities:**

* Treat **home learning during any isolation/quarantine or bubble/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 or arrange meetings with school staff or tutors
* 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
* Technology – devices and logins used at home should be used just as if hey 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

## Parents/carers

**Key responsibilities:**

* Read, sign and promote the school’s parental acceptable use policy (AUP) 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 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 changes 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.

## External groups

**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

Online Safety is taught as part of the computing curriculum and also forms part of the RSHE curriculum.

 Staff will identify opportunities to thread online safety through all school activities, 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 setting as homework tasks, all staff should encourage sensible use and consider potential dangers and the age appropriateness of websites.

We recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework ‘Education for a Connected World – 2020 edition’ from UKCIS (the UK Council for Internet Safety).

# Handling online-safety concerns and incidents

Staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, RSHE)

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.

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 on 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.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead immediately.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority’s Designated Officer).

The school will actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre’s Professionals’ Online Safety Helpline, NCA CEOP, Prevent Officer, Police). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

## Actions where there are concerns about a child

The following flow chart is taken from page 13 of Keeping Children Safe in Education 2020 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern. All concerns should be logged with the DSL. A specific form is completed for online safety. The usual safeguarding procedures will be followed.



## Sexting

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

There is a one-page overview called [Sexting; how to respond to an incident](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647389/Overview_of_Sexting_Guidance.pdf) 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, [Sexting in Schools and Colleges](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759007/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf?_ga=2.234231390.111664464.1566901980-1789411468.1557215460) to decide next steps and whether other agencies need to be involved.

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](https://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 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](https://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).

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 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.

## Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the St Margaret’s 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, we will request that the post be deleted and will expect this to be actioned promptly.

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

# Data protection and data security

There are references to the relationship between data protection and safeguarding in key Department for Education documents ‘Keeping Children Safe in Education’ and ‘Data protection: a toolkit for schools’ (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.

Rigorous control on the LGFL network firewalls and filtering all support data protection.

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.

# 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](https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring/provider-responses).

At home, school devise uses DFE Umbrella Filtering.

No pupils log into our school system on a personal device.

# 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

* We are starting to introduce pupil emails using Office 365.
* Staff at this school use Office 365.
* Both these systems are managed by SIPS IT
* To send out emails to parents we use a system called Parent Pay.
* When using Remote Learning we use email communications with parents and children through the Google Classroom and we are starting to introduce Microsoft Teams.

General principles for email use are as follows:

* Email is the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer / headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
* Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
* Staff or pupil personal data should not be sent/shared/stored on general email.
* 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.

# 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/Deputy have the day-to-day responsibility of updating the content of the website.

The DfE has determined information which must be available on a school website.

# Cloud platforms

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 following principles apply:

* 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. Levels of access to network drives are password protected.
* Pupil images/videos are only made public with parental permission
* Only school-approved platforms are used by pupils or staff to store pupil work -Office 365 and Google Classroom for RL.

# Digital images and video

When a pupil 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 displays around the school

Specific permissions are sought for any pupils to have photographs taken for public use. Any pupils shown in public facing materials are never identified with more than first name.

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. No member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on the school network in line with the retention schedule for the school Data Protection Policy.

Staff and parents are reminded 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.

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

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

# Social media

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

## 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. 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 we ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

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 [Top Tips for Parents](https://static.lgfl.net/LgflNet/downloads/digisafe/Parent-Top-Tips-Safe-Online-Corona.pdf) poster along with relevant items from parentsafe.lgfl.net and introduce the [Children’s Commission Digital 5 A Day](https://www.childrenscommissioner.gov.uk/our-work/digital/5-a-day/).

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.

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 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 .

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.

# 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)

* **Only Y6/Y5 Pupils** are allowed to bring mobile phones into school if they are walking home on their own. School seeks written permission from parents for their child to walk home alone. Devices are switched off and are then collected and kept in the school office. Any attempt to use a phone whilst on school premises will lead to the withdrawal of mobile privileges
* **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. 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 headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
* **Parents** are asked not to use their phones when entering the school building. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. Written permission is agreed for taking images at school events.

## Network / internet access on school devices

* **Pupils** are not allowed access to school networks on personal devices.
* **Home devices** when devices are issued to pupils via the DfE scheme these are restricted to the apps/software/filtering installed by the DFE. A parent agreement is signed on their use.
* **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.
* **Volunteers, contractors, governors** have no access to the school network or wireless internet on personal devices.
* **Parents** have no access to the school network or wireless internet on personal devices.

## Trips / events away from school

For school trips/events away from school, 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 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 and staff authorised by them have a statutory power to search pupil’s 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.