SACRED HEART
CATHOLIC PRIMARY
SCHOOL & NURSERY

Online Safety Policy

This is our school.

Together we worship; Together we learn; Together we belong.

With the love of God, our dreams and ambitions come true.

September 2023

Policy Date: September 2023

Policy Status: Statutory Policy

Awaiting approval by Governing Body October 2023

Review Cycle: 18months or as required

Next Review Date: January 2025

SACRED HEART
CATHOLIC PRIMARY
SCHOOL & NURSERY

SAFEGUARDING STATEMENT

“Sacred Heart Catholic Primary School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment”.

Mission Statement

This is our school.

Together we worship; Together we learn; Together we belong.

With the love of God, our dreams and ambitions come true.

Introduction

Key people/dates

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Mrs J McCallum
Deputy Designated Safeguarding Leads / DSL Team Members	Mrs Jordan Deputy DSL Mrs J Sim Deputy DSL
Link governor for safeguarding and web filtering	Mrs S Robinson
Curriculum leads with relevance to online safeguarding and their role	Mrs J Sim Curriculum Lead Mrs J Jordan PSHE/RSHE Lead Computing Lead Mr R Owen
Network manager / other technical support	Hi-Impact
Date this policy was reviewed and by whom	October 2023 – SLT and Governors
Date of next review and by whom	September 2024

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' 2023 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside Sacred Heart's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow our school's safeguarding and child protection procedures.

This policy applies to all members of the school community (staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of the school ICT systems, both in and out of school. This policy is to be followed alongside Sacred Heart's Acceptable Use Policy

Who is in charge of online safety?

KCSIE makes clear that "the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety)." The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for RSHE will plan the curriculum for their area, it is important that this ties into a whole-school approach.

What are the main online safety risks in 2023/2024?

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.

Significant risks are extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual Exploitation, criminal exploitation, serious youth violence, upskirting and persuasive/sticky design. Consensual and non-consensual sharing of nude and semi-nude images and/or videos can be signs that children are at risk.

Self-generative artificial intelligence has been a significant change, with students having often unfettered access to tools that generate text and images at home or in school. These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for information, but also in terms of plagiarism for teachers and above all safety: none of the mainstream tools have end-user safety settings, most have an age limit of 13 or even 18 and in spite of basic rude words not delivering results, will easily produce inappropriate material. School will have a responsibility to ensure sufficient procedures are being followed and that the filtering and monitoring processes are effective.

The continued cost-of-living crisis has meant that children have spent more time online and therefore exposed to all manner of online harms as families have had to cut back on leisure activities and the public provision of free activities for young people has reduced further.

Against this background, the Ofcom 'Children and parents: media use and attitudes report 2023' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further. As a school we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore remember to remind about best practice while remembering the reality for most of our students is quite different.

In 2023/2024, it is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

The Prevent Duty

The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet. The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's Computing curriculum and can also be embedded into PSHE and RSHE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

The Prevent Duty requires a schools monitoring and filtering systems to be fit for purpose.

Aims

This policy aims to:

- Set out expectations for all Sacred Heart Catholic Primary School and Nursery 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 & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online

• Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:

- for the protection and benefit of the children and young people in their care, and

- for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice

- for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession

• Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

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

Roles and responsibilities

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

We ask all children, young people and adults involved in the life of Sacred Heart Catholic Primary School and Nursery to sign an Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

The AUP is reviewed annually, and all members of the school community will be asked to sign it upon entry to the school and every time changes are made.

There are 5 AUP's these are:

1- Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS
2- Acceptable Use Policy (AUP) for VISITORS & CONTRACTORS
3- Acceptable Use Policy (AUP) for PUPILS KS1
4- Acceptable Use Policy (AUP) for PUPILS KS2
5- Acceptable Use Policy (AUP) for PARENTS/CARERS

We expect that the parents will explain the content of the policies to their child/ren to agree together and this will be outlined by the class teacher at the start of Autumn Term in “Class Meet the Teacher” welcome meetings and leaflets.

Children from Nursery to Year 6 will have these behaviour expectations and values of honesty, trust and kindness reinforced through the curriculum, teaching and learning.

Headteacher – Mrs J McCallum Key responsibilities:

- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures

- Keep updated with and share information from Local Authority Online Safety Updates

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding

- Oversee the activities of the Deputy Designated Safeguarding Leads and ensure that the DSL responsibilities listed in the section below are being followed and fully supported

- Ensure that policies and procedures are followed by all staff

- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships

- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information

- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles

- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles

- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident

- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised following The Prevent Duty

- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures

- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety

- Ensure the school website meets statutory requirements Designated Safeguarding Lead / Online Safety Lead – Mrs J McCallum Key responsibilities

- The designated safeguarding lead will take lead responsibility for safeguarding and child protection [including online safety]

- Work with the SLT and technical staff to review protections for pupils in the home and remote-learning procedures, rules and safeguards

- Ensure "An effective approach to online safety [that] empowers school to protect and educate the whole school in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate

- Liaise with staff on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies

- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns

- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply

- Work with the Headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

- Stay up to date with the latest trends in online safeguarding and undertake Prevent awareness training.

- 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.

- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance 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, but also including hard-to-reach parents.

- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.

- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.

- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine/lockdown.

- Ensure the 2017 DfE guidance on sexual violence and harassment (Updated 2021) is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying

Governing Body, led by Online Safety / Safeguarding Link Governor – Mrs S Robinson

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

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS).

- 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

- Ensure an appropriate senior member of staff, from the school, is appointed to the role of DSL [with] lead responsibility for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support.

- Support the school in encouraging parents and the wider community to become engaged in online safety activities

- Have regular strategic reviews with the online-safety co-ordinator / 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

- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex D on Online Safety reflects practice in your school

- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction.

- The training should be regularly updated in line with advice from the local three safeguarding partners, integrated, aligned and considered as part of the overarching safeguard approach.

- Ensure appropriate filters and appropriate monitoring systems are in place which do not lead to ‘overblocking’, with 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, which incorporates 'Education for a Connected World – 2020 edition'.

All staff Key responsibilities:

- Pay particular attention to safeguarding provisions for home-learning and remote-teaching technologies.

- Recognise that RSHE is a whole-school subject requiring the support of all staff; online safety has become core to this new subject. TenTen is an online platform that enhances the teaching of the RSHE curriculum

- 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 that the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) is Mrs J McCallum, Headteacher.

- Read Part 1, Annex A and Annex D 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, supporting curriculum/ Key stage/subject leads, and making the most of unexpected learning opportunities as they arise

- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place).

- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the 20 Safeguarding Principles for Remote Lessons infographic which applies to all online learning

- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.

- Be aware of security best-practice at all times, including password hygiene and phishing strategies.

- Prepare and check all online source and resources before using

- Encourage pupils 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.

- Be aware that you are often most likely to see, overhear or be alerted to online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know

- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues

- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

PSHE / RSHE Lead – Mrs J Jordan

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.

- Ensure that there is an updated RSHE policy on the school website.

- 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

- Develop, monitor and lead the use of TenTen in the teaching of the PSHE/RSHE curriculum, ensuring coverage and safe usage of the content

Computing Lead – Mr R Owen

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
- Develop, monitor and lead the use of Purple Mash in the teaching of the Computing curriculum, ensuring coverage and safe usage of the content
- Lead staff and pupils on Safer Internet Day and lead the E-Cadets on how to be ambassadors for safe online behaviour

- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school 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 and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element

Network Manager/technician – MGL

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Support the HT and DSL team as they review protections for remote-learning procedures, rules and safeguards.

- 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

- Meet the RSHE lead to see how the online-safety curriculum delivered through this new subject can complement the school IT system and vice versa, and ensure no conflicts between educational messages and practice.

- Work closely with the designated safeguarding lead / online safety lead / data protection officer to ensure that school systems and networks reflect school policy

- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms.

- 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, 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 (DPO) – Chris Walsh or Michael Jones at dpo@liverpool.gov.uk.

Key responsibilities:

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' (2021) 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 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 coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- 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 17
- 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

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.

Education and curriculum

The policy also takes into account the National Curriculum computing programmes of study.

As the use of technology and the potential risks associated with the use of the technology change rapidly, it is essential to ensure that the school community know how to use technology safely and responsibly. The school is committed to ensuring that staff receive regular training to keep up to date with new developments and ensure that they are sufficiently confident to educate pupils in the safe and responsible use of technology.
We have chosen 'Purple Mash' as an online platform to support the teaching of the Computing curriculum. Each pupil has a login and password and pupils are reminded of password privacy regularly as part of being safe online. There is a wide selection of software programmes on the platform to teach the children effectively under the restrictions of an age appropriate, secure network.

The curriculum is reviewed and revised on a regular basis to ensure that it remains current. The school will also endeavour to provide information and training opportunities for parents and carers to raise their awareness of the technologies that their children are potential using and the risks that they potentially face.

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

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc.) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites. The use of Purple Mash will minimise the use of other unregulated platforms as it has the appropriate tools and software needed to develop the children's education.

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

At Sacred Heart Catholic Primary School and Nursery, 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).

Online Safety is woven into our PSHE curriculum and pupils are regularly given Online Safety lessons to ensure pupils are regularly checking their practices online.

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

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place). "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 2023).

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

At Sacred Heart Catholic Primary School and Nursery, 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

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE
School procedures for dealing with online-safety are detailed in the following policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Prevent Policy
- Data Protection Policy

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 through the school's escalation processes.

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

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). 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, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

Examining electronic devices

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.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on Searching, screening and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

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).

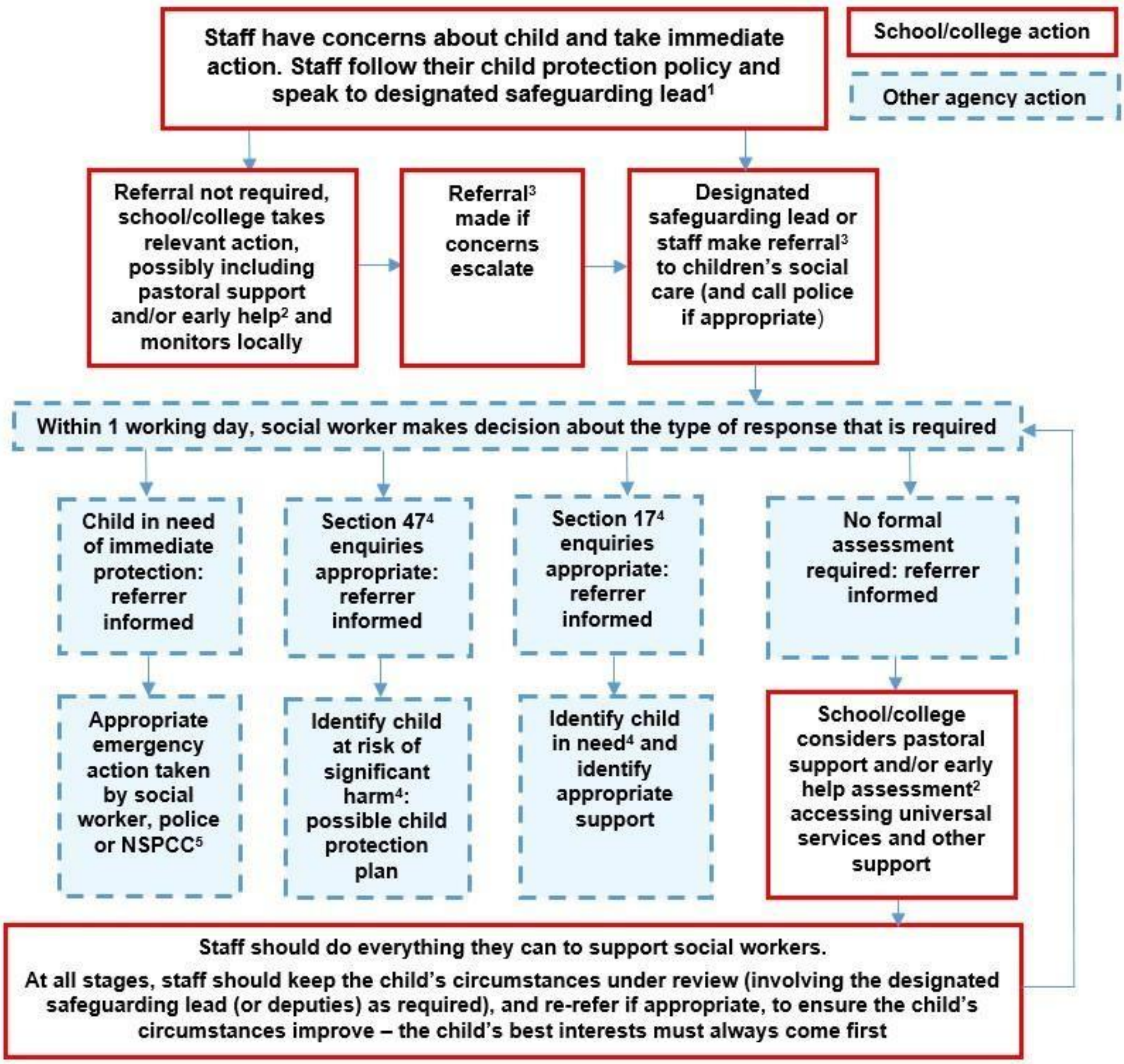
These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

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

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.

Actions where there are concerns about a child

The following flow chart is taken from page 23 of Keeping Children Safe in Education 2021 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern


Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2] and monitors locally
Referral[3] made if concerns escalate
Designated safeguarding lead or staff make referral[3] to children's social care (and call police if appropriate)
Within 1 working day, social worker makes decision about the type of response that is required
Child in need of immediate protection: referrer informed
Section 47[4] enquiries appropriate: referrer informed
Section 17[4] enquiries appropriate: referrer informed
No formal assessment required: referrer informed
Appropriate emergency action taken by social worker, police or NSPCC[5]
Identify child at risk of significant harm[4]: possible child protection plan
Identify child in need[4] and identify appropriate support
School/college considers pastoral support and/or early help assessment[2] accessing universal services and other support
Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

Sexting

Sacred Heart Catholic Primary School and Nursery refers to the UK Council for Internet Safety (UKCIS) guidance on sexting in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

The term 'sexting' describes the use of technology to share personal sexual content. It's a word-mix of sex and texting. The content can vary, from text messages to images of partial nudity to sexual images or video. This content is usually created to be sent to a partner, but can be between groups and can use a range of mobile devices, technologies and online spaces. Photos and videos are often created via webcam or smartphone camera, and are shared on social networking sites such as Facebook, Twitter, Tumblr, Snapchat, Flickr and video sites such as YouTube.

Sharing photos and videos online is part of daily life for many people, enabling them to share their experiences, connect with friends and record their lives. This increase in the speed and ease of sharing imagery has brought concerns about young people producing and sharing sexual imagery of themselves. This can expose them to risks, particularly if the imagery is shared further, including embarrassment, bullying and increased vulnerability to sexual exploitation. Producing and sharing sexual images of under 18s is illegal.

Although the production of such imagery is more than likely to take place outside of school we need to be able to respond swiftly and confidently to ensure that all children are safeguarded, supported and educated.
These procedures are part of the school's safeguarding arrangements and all incidents of youth produced sexual imagery will be dealt with as safeguarding concerns and will be responded to in line with the school's safeguarding and child protection policy.

A one-page overview called Sexting; how to respond to an incident is displayed in the staff room 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.

Sacred Heart's DSL will in turn use the full guidance document, Sexting in Schools and Colleges to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.
The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

Sacred Heart Primary School and Nursery 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 2021. Pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying and Cyberbullying

Online bullying in treated like any other form of bullying and our school bullying policy is followed for online bullying, which may also be referred to as cyberbullying, including issues arising from messaging, social media and online platforms.
Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education 2021 and Sexual Violence and Sexual Harassment 2021. It would be useful for all staff to be aware of this guidance: paragraphs 45-50 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. This can include behaviours such as bra-strap flicking and the careless use of language.

If pupils find that they have accessed content online that is of a sexual nature and is concerning for child exploitation, they are taught to report it to a trusted adult, CEOP or NSPCC.

Social media

Sacred Heart has rules and expectations of behaviour for children and adults in the Sacred Heart Catholic Primary School and Nursery community whilst accessing Social Media. These are also governed by school Acceptable Use Policies. Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff and Parents/Carers).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Sacred Heart Catholic Primary School and Nursery 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. If the post threatens the safety of a pupil, staff member or member of the community, the Police will be contacted.

Pupils are not permitted to use social networking sites within school. Pupils and families are regularly directed to information on age restrictions for applications and networking sites.

Whilst we aim to promote the School and understand it is key to reputational value, we follow Online Safety principles at all times. SLT, are responsible for managing our X (Twitter) accounts. Online Safety Boost at SWGFL monitor school's online reputation and reports this to the Headteacher.

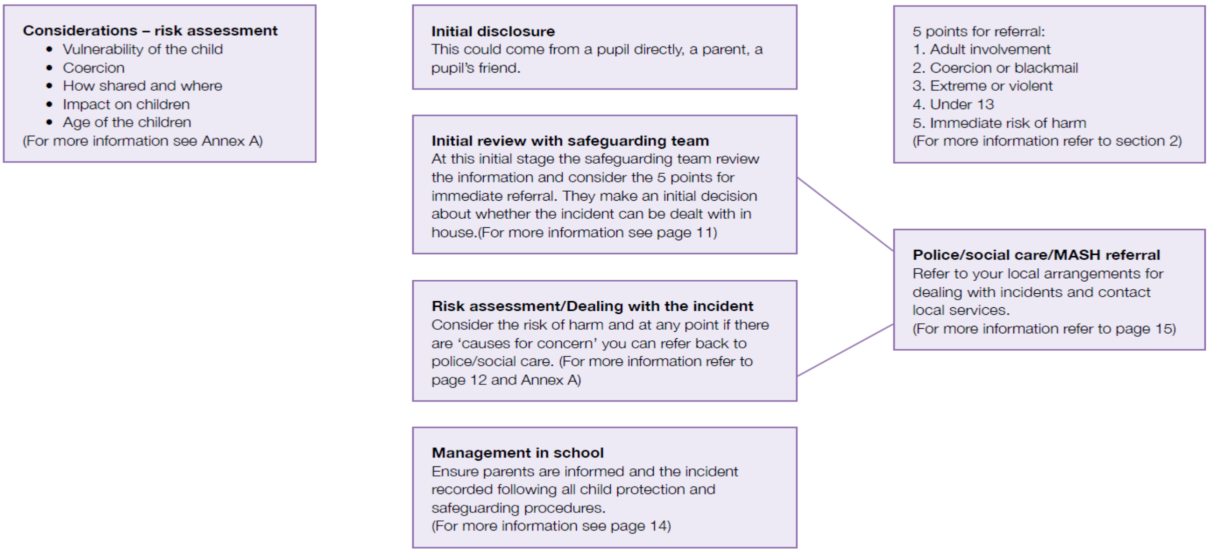
Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the Acceptable Use policies which all members of the school community sign, 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. 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 will be dealt with according to our reporting policy. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

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

Staff are reminded to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should not accept friend requests from pupils on social media platforms.

Annex G

Flowchart for responding to incidents



Considerations – risk assessment

- Vulnerability of the child
- Coercion
- How shared and where
- Impact on children
- Age of the children

(For more information see Annex A)

Initial disclosure
This could come from a pupil directly, a parent, a pupil's friend.

Initial review with safeguarding team
At this initial stage the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house.(For more information see page 11)

Risk assessment/Dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you can refer back to police/social care. (For more information refer to page 12 and Annex A)

Management in school
Ensure parents are informed and the incident recorded following all child protection and safeguarding procedures.
(For more information see page 14)

5 points for referral:
1. Adult involvement
2. Coercion or blackmail
3. Extreme or violent
4. Under 13
5. Immediate risk of harm

(For more information refer to section 2)

Police/social care/MASH referral
Refer to your local arrangements for dealing with incidents and contact local services.
(For more information refer to page 15)

Data protection and data security

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

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements, which are available from the school office.

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 Egress to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

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 home, school devices are Chrome Books which are linked to our school's Google domain. This allows us to track pupil activity. Parents will sign an Acceptable User's agreement prior to being loaned a Chrome book. Any inappropriate content discovered will be dealt with in line with the usual safeguarding procedures.

At Sacred Heart, the internet connection is provided by MGL. This means we have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security, including a web filtering system called Smooth wall.
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

The school network provides a level of filtering and monitoring that supports safeguarding. The school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending appropriate awareness training/online safety lessons.

If staff or pupils discover an unsuitable site, it must be reported to the OSL immediately. If users discover a website with potentially illegal content, this should be reported immediately to the DSL and OSL. The school will report such incidents to appropriate agencies including Internet Service Provider (ISP), Police, CEOP or the Internet Watch Foundation (IWF).

Any amendments to the school filtering policy or block and allow lists will be checked and assessed by the Headteacher/OSL prior to being released or blocked. The impact of the Online Safety policy and practice is monitored through the review / audit of online safety incident logs, behaviour / bullying logs, surveys of staff, students /pupils, parents / carers.

Email

General principles for email use are as follows:

- Google Classroom, virtual learning environment and Class Dojo (for pupils in EYFS) are the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer / Headteacher in advance. X (Twitter) is accessed by all staff so responses to messages must be authorised 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).

- Staff at this school use the Mail 365 system for all school emails

Staff or pupil personal data should never be sent/shared/stored on email. If data needs to be shared with external agencies the Egress system will be used.

- 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 day-to-day responsibility of updating the content of the website is managed by SLT. The site is managed by Hi-Impact.
- Where other staff submit information for the website, they are asked to remember:
  - School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. If in doubt, check with Mrs J McCallum, Headteacher.
  - Where pupil work, images or videos are published on the website, their identities are protected and full names are not published.

Cloud platforms

Microsoft's Office 365 and Google for Education's G Suite are used as School 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:

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

Digital images and video

- Using photographs and videos to evidence the children's learning is encouraged as part of our assessment strategies. It is also a vital part of communication with parents and strengthening the home-school link.
- When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos to be

used on Sacred Heart Catholic Primary School and Nursery website and social media accounts X(Twitter).

- Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.
- Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).
- All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Sacred Heart Catholic Primary School and Nursery 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 of the school Data Protection Policy.
- Staff and parents are reminded regularly about the importance of not sharing images/videos without permission, due to reasons of child protection data protection, religious or cultural reasons, or simply for reasons of personal privacy. Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.
- We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing.
- 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
- Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission.
  - We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location.

- We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse. This includes consensual and non-consensual sharing of nude and semi-nude images and/or videos.

Mobile phones and other devices

- At Sacred Heart, we recognise that there are times that staff will need access to mobile phones during the working day. However, the usage needs to adhere to the following regulations. We also accept that pupils may have their own mobile device and they must follow school rules.
- Pupils in Y5/6 are allowed to bring mobile phones into school for use when they are coming to school and walking home. The mobile phone must be given to office staff as soon as the child enters school and can be collected at the end of the school day. Children are not allowed to use their mobile phone during school time. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to the mobile phone being confiscated. Parents will be contacted about this and further action may be taken.
- 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. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they should seek permission for this from the Headteacher. Any phone call should then be used in the private staff areas.

- **Volunteers, contractors, governors** should leave their phones in their pockets and turned on silent. 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.
- **Parent** should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children.

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

Emergencies – Staff are instructed that they can use their mobile phone in the event of an emergency and as part of the 'Lockdown Policy'.

Keeping devices secure

- All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:
- Keeping the device password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters.
- Ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device lock if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing antivirus and anti-spyware software.
- Keeping operating systems up to date – always install the latest updates.