



SACRED HEART
CATHOLIC PRIMARY
SCHOOL & NURSERY

Online Acceptable Use 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



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.



Background and Rationale

INTRODUCTION

A school collects, hold and uses information that is both confidential and valuable. Such information and the computer systems that store, process and transmit it must be adequately protected against any activity that could affect authorised and lawful use.

It is also important that the use of ICT resources is regulated, to ensure that a school complies with relevant legislation, regulatory codes of practice, its own governance arrangements and ICT & Information Security best practice. This policy has been developed to set standards and provide users with clear instructions and guidance on what constitutes acceptable and unacceptable use. Should issues arise, staff and head teachers may wish to liaise with trade unions at an early stage, who can provide guidance documents with specific scenarios which may be helpful.

In brief, the aims of the Acceptable Use Policy (AUP) are to:

- Protect School staff, users and the School's equipment and the information assets we hold;
- Prevent the abuse or misuse of computer, internet, e-mail facilities and paper files;
- Prevent information security incidents and/or information loss and breaches;
- Ensure compliance with legislation;
- Where applicable, protect the Councils ICT Facilities.

This policy should be read in conjunction with the relevant School's policies, procedures and guidance.

Key Message

All users must be aware of their obligations under this policy and take reasonable action to ensure on-going compliance.

As a condition of use, it is the responsibility of users to ensure that they keep up-to-date with the latest requirements of the policy.

Who does the Acceptable Use Policy apply to?

This policy and any references to 'the school' or 'users' refer to, but are not limited to, teachers and all other school staff, agency workers, contractors, 3rd parties and temporary staff such as work placements.

Responsibilities of Head Teachers & Governors

Head Teachers and/or Governors will support this AUP by:

- Implementing the Policy within the school and ensuring that the AUP is circulated to all personnel;
- Ensuring that staff understand the legal risk and security implications of improper use of school ICT facilities;
- Promoting good information security practice, by leading by example and ensuring they adhere to the conditions within this policy;
- Defining, with their team, the acceptable level of personal use of school and personally owned hardware such as mobile phones and facilities such as personal email accounts etc.

Head Teachers and/or Governors must ensure that the ICT facilities utilised by their school are configured and operated appropriately to protect the information held within or accessed by them.

Privacy, Monitoring and Filtering

Right to Privacy

It is accepted that the private lives of employees can, and usually will extend into the workplace. Consequently, to ensure your right to privacy, all monitoring activities will be governed by the Data Protection Act 2018 and the Human Rights Act 1998.

All reasonable measures will be undertaken to ensure that personal emails marked as such will not be opened in the course of monitoring unless there is a legal requirement to do so or there is suspicion that email has been used in a way that would constitute gross misconduct under their contract of employment.

Monitoring

The School (and/or Council if applicable) does not generally engage in systematic monitoring and recording activities. However, it reserves the right to do so where there is reason to believe that misuse of its information assets or computing facilities is occurring.

Nevertheless, the school (and/or Council if applicable) maintains the right to examine any systems and inspect any data recorded in those systems. In order to ensure compliance with this policy, the school (and/or Council if applicable) also reserves the right to use monitoring software in order to check upon the use and content of emails.

Key Message

Any individual using the information assets or computing facilities of the school consents to such monitoring and recording. If apparent criminal activity is detected, monitoring logs, in conjunction with specific personal information, may be provided to the Police.

Such monitoring is for legitimate purposes only and will be undertaken in accordance with the procedure agreed with employees.

Filtering

For Schools taking the Council's e-mail and Internet services, they are both automatically filtered to ensure that inappropriate and unauthorised content is minimised as far as is possible without detracting from either service.

General Principles

The School's ICT facilities must only be used by those authorised to do so. Any user who requires access to School ICT facilities must first:

- Be authorised to do so by a manager or supervisor;
- Read, understand and accept all relevant School policies and this Acceptable Use Policy.
- You must not deliberately or knowingly use the School's ICT facilities to view, copy, create, download, share, store, print, e-mail, transfer or otherwise access any material which:
 - Is sexually explicit or obscene;
 - Is racist, sexist, homophobic or in any other way discriminatory or offensive;
 - Contains content where the possession, transmission or sharing of would constitute a criminal offence;
 - Promotes any form of criminal activity;
 - Brings the School into disrepute and/or exposes it to legal action.

It is unacceptable to use the Schools ICT facilities to:

- Conduct any non-approved business;
- Undertake any activities detrimental to the reputation of the School;
- Make offensive or derogatory remarks about anybody on social media or otherwise via the Internet or e-mail;
- Create, transmit, download or share information, or install software or applications, which would breach copyright, confidentiality or any other applicable legislation;
- Impersonate or attempt to impersonate another individual or organisation;

- Attempt to gain access to information or information systems you are unauthorised to access;
- Attempt to bypass internet filtering or any monitoring functions;
- Attempt to conceal your identity by using anonymising software or services;
- Deliberately or knowingly undertake activities that corrupt or destroy School data, disrupt the work of others, deny network resources to them or violate the privacy of other users.

Key Message

Communicating with both current and former pupils via social networking sites or via other non-school related mechanisms such as personal e-mails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role.

Adults should ensure that all communications are transparent and open to scrutiny.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming.

They should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers. Communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations.

This also includes communications through internet based web sites.

Use of school ICT equipment

Any equipment supplied to you (for example, Laptops, PCs, Smartphones, Tablets) remains the property of the School at all times, with the user assuming temporary 'custodianship'.

Do's

- Make sure that at all times you use this equipment in accordance with this Acceptable Use Policy, securely, for the purpose for which it was issued to you, without reconfiguration and in compliance with relevant legislation such as the Computer Misuse Act 1990 and Data Protection Act 2018
- On leaving employment with the School, you must ensure that all ICT equipment is returned to your line manager or the Head Teacher;
- Before you store any films, music or other media on ICT equipment, ensure that you are aware of your responsibilities under the current intellectual property legislation.
- Report the loss or theft of any ICT equipment to your school;
- Ensure that your screen cannot easily be viewed by others when accessing sensitive information. For example, if you were working away from Schools premises or in a public area.

Safety of Equipment Off Site: Laptop, Tablet and Smartphone Users

All School ICT equipment is subject to information security risks, but the portability of laptops, tablets and smartphones makes them particularly vulnerable to damage, loss or theft, either for their re-sale value or the information they contain. When outside of secured premises, there is an increased risk to any laptops or portable devices that you may carry as part of your role.

Do's

- Users must keep ICT equipment in their possession within their sight whenever possible. ICT equipment should never be left visibly unattended unless it is suitably secured.
- Extra care should be taken in public places such as airports, railway stations or restaurants;
- When transporting ICT equipment, you should look to minimise the risk of loss or theft. For example, putting a laptop out of sight in the boot of a car rather than on the passenger seat;
- You must ensure that the device is regularly connected and logged onto the network to receive its security updates;
- You must ensure that laptops are regularly restarted to ensure that all security updates are applied;
- Any data saved to the device is not backed up centrally. You should avoid saving data to the device wherever possible. However, where this is necessary for operational reasons you must ensure that data on the device is backed up to the network storage areas for your School as soon as is practical.

Don'ts

- If a device is secured either with an encryption password or a 'lock screen' password, you must not share your encryption / lock screen password with anyone or write this down.
- Devices taken off site must contain a passcode or encryption or password protection.

Personal Use of School Equipment & ICT Facilities

Improper or inappropriate personal use of the School's/Council's e-mail and Internet systems may result in disciplinary action.

School devices contain or enable access to school data and systems. Personal use of school ICT equipment does not extend to other family members, friends or any other person.

Secure Disposal of School ICT Equipment

School ICT equipment which is broken, no longer fit for purpose, redundant or to be used/donated for other purposes should be securely wiped (where applicable) and disposed in-line with WEEE regulations.

Don'ts

- You must not sell or donate School equipment to staff, charities or any other third- parties without the explicit authorisation of the Head Teacher and/or the School Governors.

Use of personal and non-school ICT equipment

The use of non-school and personal ICT equipment to undertake school business brings both opportunities and risks. The potential for an increase in flexibility and convenience must be balanced against the need to keep personal and sensitive information secure.

- You must only use your personal hand held/external devices (mobile phones/USB devices etc.) in School if permission has been gained from the Headteacher. Employees must understand that, if they do use their own devices in School, they will follow the rules set out in this agreement, in the same way as if they were using School equipment;
- You must keep personal phone numbers and email accounts private and not use your own mobile phones or email accounts to contact pupils;
- You must only use a School mobile phone when on a school trip
- See Personal Mobile and Devices Policy

Social Media

Although this Acceptable Use Policy applies to the use of School facilities, it is important to note that the use of social media outside of work can affect the workplace. For example:

- Comments posted on social media may be seen by work colleagues, and a private disagreement may 'spill over' into the workplace.
- You must not use social networking sites to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages.
- You must not befriend pupils or ex pupils under the age of 18 on social networking sites.
- It is advised not to befriend/follow family members of pupils, governors, clergy, ex pupils or ex parents on social media. Staff should consider carefully the implications of this;
- Do not post information and photos about yourselves, or School-related matters, publicly that you wouldn't want employers, colleagues, pupils, parents and other School stakeholders to see;
- Do not mention the school by name in any personal social media profile or online profile

Security Incidents

Security Incidents, for example the theft of a laptop, a computer virus or a successful hacking attack could compromise the security of School. A successful compromise may:

- Affect business operations;
- Lead to financial loss or reputational damage;
- Be a threat to the personal safety or privacy of an individual or organisation;
- Need to be reported to the UK Government, the Information Commissioner's Office, Police or a number of other organisations.

Do's

Ensure you report all security incidents to the school and Hi-Impact to secure your device from hacking.

Don'ts



Don't ignore a security incident assuming that someone else will report it.



KS1 Acceptable User

My name is _____

To stay **SAFE online and on my devices**:

1. I only **USE** devices or apps, sites or games if I am allowed to
2. I **ASK** for help if I'm stuck or not sure; I **TELL** a trusted adult if I'm upset, worried, scared or confused
3. I look out for my **FRIENDS** and tell someone if they need help
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I **KNOW** that online people aren't always who they say they are and things I read are not always **TRUE**
6. Anything I do online can be shared and might stay online **FOREVER**
7. I don't keep **SECRETS**  unless they are a present or nice surprise
8. I don't have to do **DARES OR CHALLENGES** , even if someone tells me I must
9. I don't change **CLOTHES** or get undressed in front of a camera
10. I always check before **SHARING** my personal information or other people's stories and photos
11. I am **KIND** and polite to everyone

✓

My trusted adults are:

_____ **at school**

_____ **at home**



KS2 Acceptable User Policy

These statements can keep me and others safe & happy at school and home

1. ***I learn online*** – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.
2. ***I behave the same way on devices as face to face in the classroom, and so do my teachers*** – If I get asked to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am creative online*** – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things, remembering my 'Digital 5 A Day'.
5. ***I am a good friend online*** – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am not a bully*** – I know just calling something fun or banter doesn't stop it maybe hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
7. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
8. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I

know it is safe or has been agreed by trusted adults.

Sometimes app add-ons can cost money, so it is important I always check.

9. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it

10. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult.

11. ***If I make a mistake I don't try to hide it but ask for help.***

12. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.

13. ***I know online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.

14. ***I never pretend to be someone else online*** – it can be upsetting or even dangerous.

15. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.

16. ***I don't go live (videos anyone can see) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

17. ***I don't take photos or videos or people without them knowing or agreeing to it*** – and I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.

18. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

19. **I say no online if I need to** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.

20. **I tell my parents/carers what I do online** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

21. **I follow age rules** – 13+ games, apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.

22. **I am private online** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.

23. **I am careful what I share and protect my online reputation** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).

24. **I am a rule-follower online** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.

25. **I am part of a community** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.

26. **I respect people's work** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.

27. **I am a researcher online** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, and I know which sites to trust, and how to double check information I come across. If I am not sure I ask a trusted adult.

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult:

At school that might mean _____

Outside school, my trusted adults are _____

I know I can also get in touch with [Childline](#).

Signed: _____

Date: _____



Staff Acceptable User Policy

Background

We ask everyone 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).

This AUP is reviewed annually, and staff, governors and volunteers are asked to sign it when starting at the school and whenever changes are made. All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy. If you have any questions about this AUP or our approach to online safety, please speak to Mrs McCallum (Headteacher, DSL), Mrs Jordan (Deputy Headteacher, DDSL) or Mrs Sim (Assistant Headteacher, DDSL)

What am I agreeing to?

I have read and understood Sacred Heart Catholic Primary School's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay as outlined in the Online Safety Policy.

1. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area. I have noted the section in our online

safety policy which describes trends over the past year at a national level and in this school.

2. I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult) and make them aware of new trends and patterns that I might identify.
3. I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media)
4. I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom. understand the sections on.
5. I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment.
6. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language
7. I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).
8. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).

9. I will follow best-practice pedagogy for online-safety education, avoiding scaring and other unhelpful prevention methods.
10. I will prepare and check all online sources and classroom resources before using for accuracy and appropriateness. I will flag any concerns about overblocking to the DSL/DDSL.
11. I will 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 data protection.
12. During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.
13. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
14. I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE 2023, now led by the DSL. If I discover pupils may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.
15. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

16. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the Headteacher.
17. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am ever not sure, I will ask first.
18. I agree to adhere to all provisions of the school's Cybersecurity and Data Protection Policies at all times, whether or not I am on site or using a school device, platform or network.
19. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
20. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.
21. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
22. I understand that breach of this AUP and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

To be completed by approver:

I approve this user to be allocated credentials for school systems as relevant to their role.

Signature: _____

Name: _____

Role: _____

Date: _____



Parent Acceptable User Policy

Background

We ask all children, young people and adults involved in the life of Sacred Heart Catholic Primary School and Nursery to read and sign an Acceptable Use Policy (AUP) to outline 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).

Your child has also signed an AUP which you can find on our website in the Acceptable Use Policy. We tell your children that **they should not behave any differently when they are out of school or using their own device or on a home network.** What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school. We seek the support of parents and carers to reinforce this message and help children to behave in a safe way when online:

“Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face.”

Where can I find out more?

You can read Sacred Heart Catholic Primary's full Online Safety Policy at <https://www.sacredheartliverpool.school/policies> for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding and Child Protection Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to Mrs McCallum (Headteacher, DSL), Mrs Jordan (Deputy Headteacher, DDSL) or Mrs Sim (Assistant Headteacher, DDSL).

What am I agreeing to?

1. I understand that Sacred Heart Catholic Primary School and Nursery uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the

smooth running of the school, and to help prepare the children and young people in our care for their future lives.

2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including through behaviour policies and agreements, physical and technical monitoring, education and support and web filtering.
3. School network protections will be superior to most home filtering. However, please note that accessing the internet always involves an element of risk and the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies. Schools are asked not to overblock or provide an experience which is so locked down as to block educational content or not train pupils for life in an online world.
4. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school is subject to filtering and monitoring. More detail of this can be found in our online safety policy.
5. I understand and will help my child to use any devices at home in the same manner as when in school, including during any remote learning periods.
6. I will support my child to follow the school's policy regarding bringing devices to school. Pupils are not to bring devices into school without permission from the Headteacher.
7. I understand that my child might be contacted online on Purple Mash and only about their learning, wellbeing or behaviour. If they are contacted by someone else or staff ask them to use a different app to chat, they will tell another teacher (Mrs McCallum DSL).
8. I will promote positive online safety and model safe, responsible and positive behaviours in my 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.

9. Parents are kindly asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.
10. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
11. I will follow this policy which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
12. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety and refer to parentsafe.lgfl.net for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screen time and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc...
13. I understand that my child needs a safe and appropriate place to do home learning, whether for homework or during times of school closure. When on any video calls with school, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
14. If my child has online tuition, I will refer to the Online Tutors – Keeping children Safe poster and undertake necessary checks where I have arranged this privately, ensuring they are registered/safe and reliable, and for any tuition to remain in the room where possible, ensuring my child knows that tutors should not arrange new sessions or online chats directly with them.

15. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet and to various devices, operating systems, consoles, apps and games. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content. Find out more at parentsafe.lgfl.net
16. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my child, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
17. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and which can be seen here <https://www.sacredheartliverpool.school/policies> and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
18. I can find out more about online safety at Sacred Heart Catholic Primary School and Nursery by reading the full Online Safety Policy here <https://www.sacredheartliverpool.school/policies> and can talk to Mrs McCallum (Headteacher, DSL), Mrs Jordan (Deputy Headteacher, DDSL) or Mrs Sim (Assistant Headteacher, DDSL) if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian _____

Parent / guardian of: _____

Date: _____



Visitors and Contractors Acceptable Use Policy

Background

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.

Visitors and contractors are asked to sign this document before they are allowed access to the school or its pupils. Many of these rules are common sense – if you are in any doubt or have questions, please ask the DSL Mrs McCallum or the DDSLs, Mrs Jordan and Mrs Sim.

Further details of our approach to online safety can be found in the overall school Online Safety Policy

<https://www.sacredheartliverpool.school/policies>

If you have any questions during your visit, you must ask the person accompanying you (if appropriate) and/or Mrs McCallum (DSL) or the DDSLs, Mrs Jordan and Mrs Sim.

What am I agreeing to?

1. I understand that any activity on a school device or using school networks, platforms, internet and logins may be captured by one of the school's security, monitoring and filtering systems and/or viewed by an appropriate member of staff.
2. I will never attempt to arrange any meeting with a pupil, 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.
3. I will leave my phone in my pocket and turned off. Under no circumstances will I use it (or other capture device) in the

presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students. If required (e.g. to take photos of equipment or buildings), I will have the prior permission of the Headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff.

4. If I am given access to school-owned devices, networks, cloud platforms or other technology:
 - I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use
 - I will not attempt to access any pupil / staff / general school data unless expressly instructed/allowed to do so as part of my role
 - I will not attempt to make contact with any pupils/students or to gain any contact details under any circumstances
 - I will protect my username/password and notify the school of any concerns
 - I will abide by the terms of the school Data Protection Policy protections <https://www.sacredheartliverpool.school/policies>
 - I understand that my online activity will be subject to the school's filtering and monitoring systems, and that any attempts to access content which is illegal or inappropriate for a school setting, may result in further action as per the safeguarding procedures and may result in termination of contract.
5. I will not share any information about the school or members of its community that I gain as a result of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the school.
6. I will not reveal any information on social media or in private which shows the school in a bad light or could be perceived to do so.
7. I will not do or say anything to undermine the positive online safety messages that the school disseminates to pupils/students and will not give any advice on online safety

issues unless this is the purpose of my visit and this is pre-agreed by the school. NB – if this is the case, the school will ask me to complete Annex A and consider Annex B of '[Using External Visitors to Support Online Safety](#)' from the UK Council for Child Internet Safety (UKCIS).

8. I understand that children can be abused and harmed when using devices and I will report any behaviour (no matter how small) which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult). Mrs McCallum (DSL), Mrs Jordan (DDSL) or Mrs Sim (DDSL).
9. I will only use any technology during my visit, whether provided by the school or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance. I will not view material which is or could be perceived to be inappropriate for children or an educational setting.
10. I will behave in a professional and responsible manner at all times and understand that failure to do so may result in further action being taken and could result in the termination of my contract.

To be completed by the visitor/contractor:

I have read, understood and agreed to this policy.

Signature/s: _____

Name: _____

Organisation: _____

Visiting / accompanied by:

Date / time: _____

To be completed by the school (only when exceptions apply):

Exceptions to the above

policy: _____

Name / role / date / time: _____