

Sacred Heart
Catholic Primary School



Learning in Love

Acceptable Use of IT Agreements 2026-28

Mission Statement

Guided by truth, respect and compassion; we share in building upon every individual's foundation, nurturing a love of learning in preparation for tomorrow's society, with Jesus at the heart of all we do.

Governing Body with Responsibility	Resources
Agreed by Governors on	
Chair's Signature	
Staff Member Responsible for Review	School Business Manager
Date for Review	June 2028

What is an Acceptable Use Policy (AUP)?

We ask all children, young people and adults involved in the life of Sacred Heart Catholic Primary School 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 uses the latest LGfL AUP templates (see below) and will be reviewed every 2 years. People will be asked to sign it on joining the school and at the start of each academic year.

AUP: Staff, Governors and Volunteers (updated February 2026)

AUP: Parents and carers (updated September 2025)

AUP: Key Stage 1 Pupils (updated September 2025)

AUP: Key Stage 2 Pupils (updated September 2025)

AUP: Visitors and Contractors (updated September 2025)

AUP: Symbols for pupils with SEND (updated September 2025)

Why do we need an AUP?

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.

Where can I find out more?

All staff, governors and volunteers should read Sacred Heart Primary's full [Online Safety Policy](#) for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, Social Media Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to the Headteacher.

Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS

We ask everyone involved in the life of Sacred Heart Catholic Primary School 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 every two years, and staff, governors and volunteers are asked to read, understand, follow and sign it when starting at the school and at the start of each academic year or 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, it is your responsibility to please speak to the Headteacher.

What am I agreeing to?

1. (This point is for staff and governors):

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.

2. 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.

3. I will report any behaviour which I believe may be inappropriate or concerning in any way (by adults or pupils) to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult) and make them aware of new trends and patterns that I identify.

4. I will uphold the reputation of the school at all times and 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).

5. 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.

6. 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 – know that 'it could happen here'! If I am unsure how to address any issues, I will seek support from the DSL.

Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS

7. I will follow the school's policy on use of mobile phones/devices at school and only use in staff areas. I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff without permission from the Senior Leadership Team. Where I do use personal equipment to take a photograph, this will be done in the presence of another member of staff and I will transfer any such images or videos to a school drive at the first possible opportunity and will delete them from my own device. The same principles apply for wearable technology. Smart glasses must not be worn in school. Please speak to the Headteacher if this presents any issue.
8. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.
9. 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).
10. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk with pupils 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).
11. I will check with the School Business Manager if I want to use any new platform or app that has not already been approved by the school, to ensure this is quality assured. This includes any generative AI apps.
12. I will follow best-practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods.
13. I will prepare and check all online sources and classroom resources before using them, for accuracy and appropriateness (including ensuring adverts do not play at the beginning of videos). I will flag any concerns about "overblocking" to the DSL (such as if I cannot access teaching materials).
14. 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.
15. I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.
16. 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.
17. 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

Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS

(regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

18. 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. If I discover pupils or adults 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.

19. I will maintain a professional presence online and carefully consider how I interact with our schools'/school's communities. I understand that all communication must be conducted by official school channels and communication platforms to maintain professional standards and data security. I will not use any personal email, WhatsApp or social media for school purposes unless there is explicit agreement by school leaders.

20. 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.

21. I will review my personal social media privacy settings regularly to make sure I am happy with information about me that is publicly available.

22. 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.

23. If I already have a personal relationship with a pupil or their family, I will inform the DSL/Headteacher of this as soon as possible.

24. 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.

25. I will not use any new technology or download any apps without agreement from the School Business Manager

26. I will not use a mobile hotspot to provide internet to any device I use in school.

27. I agree to adhere to all provisions of the school's [Data Protection](#) Policy at all times, whether or not I am on site or using a school device, platform or network.

28. 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.

29. 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

Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS

offensive or of an extremist nature. I understand that any breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

30. I will only use AI platforms that have been authorised for use (including those used with pupils and to support administrative tasks), and I will ensure that any use of these platforms is transparent, responsible, appropriate, legal and ethical. I will ensure that I abide by all data protection legislation and the school's [AI Policy](#) in relation to using these platforms.

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 the Headteacher

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

Signature: _____

Name: _____

Role: _____

Date: _____

Acceptable Use Policy (AUP) for **PARENTS & CARERS**

The use of technology is an essential part of all of our lives. At Sacred Heart Catholic Primary School we take our responsibilities for supporting your child to develop skills in using technology very seriously, and their safety and wellbeing are our utmost priority to us.

We ask all children, young people and adults involved in the life of Sacred Heart 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 will sign an AUP which will be kept in the front of their IT Folder. 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’s full [Online Safety Policy](#) for more detail on our approach to online safety. Other relevant (eg Safeguarding and Child Protection Policy, Behaviour Policy, etc are available on our website). If you have any questions about this AUP or our approach to online safety, please speak to the Headteacher.

What am I agreeing to?

1. I understand that Sacred Heart 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.

Acceptable Use Policy (AUP) for PARENTS & CARERS

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 (mobile phones, tablets, Smart watches and glasses etc) to school. From September 2026 children will not be allowed to bring a Smartphone into school. Only Year 6 children who walk independently to and from school are allowed to bring in a phone and this must be turned off and handed in to their teacher during the school day.
7. I understand that my child might be contacted online through Google Classroom by a class teacher, Phase Leader or member of the school's Senior Leadership Team. This will only be about their learning. If they are contacted by someone else or staff ask them to use a different app to chat, please report this to the Headteacher.
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. 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 will not encourage my child to join any platform where they are below the minimum age (for nearly every social media platform, this means under 13 years old).
10. When I visit the school premises, I will keep any online technology in my pocket wherever possible.
11. I will follow the guidance from the school about 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 (see [nofilming.lgfl.net](#) for more information). 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 Arbor.
12. I will not covertly film or make recordings of any interactions with pupils or adults in schools. If I wish to make any recording, we request you to please speak to the Headteacher.
13. 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, screentime and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc.

Acceptable Use Policy (AUP) for PARENTS & CARERS

14. Research tells us that the majority of children are now accessing artificial intelligence in some form, which is available for free on most mainstream apps and social media platforms. There are some significant risks involved with this including talking to chatbots, and the use of nudifying apps and image creators to create inappropriate and illegal images/videos I will talk to my child about these risks. Find out more at parentsafe.lgfl.net

15. I understand that whilst home networks are much less secure than school ones, I can apply safety settings to my home internet and to various devices, operating systems, consoles, apps and games. Find out more at parentsafe.lgfl.net

16. There are also child-safe search engines e.g. [swiggle.org.uk](https://www.swiggle.org.uk) and YouTube Kids is an alternative to YouTube with age appropriate content. I can also set up SafeSearch to filter explicit content from searches.

17. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my child, role model healthy behaviours and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/

18. I will not attempt to track my child during the school day or on school trips, eg with Apple AirTags or similar devices. Not only is this against the terms and conditions of these products, it is unhelpful to the operation of the school, can broadcast the location of children to passing users and can lead to unnecessary distress among parents eg if a school trip has an unannounced change of route or schedule.

19. 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 below in this document. I understand that s/he may be subject to sanctions if s/he does not follow these rules.

20. I can find out more about online safety at Sacred Heart by reading the full [Online Safety Policy](#) and can talk to my class teacher, Phase Leader, ICT Lead 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:

Please note that parents may also be interested in the school's approach to online safety, which are is covered in our [Online Safety Policy](#).

Acceptable Use Policy (AUP) for **CHILDREN (KEY STAGE 1)**

My name is _____

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

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

✓

My trusted adults are:

_____ at school

_____ at home

_____ at _____ (eg place of worship, club, childminder)

Acceptable Use Policy (AUP) for **CHILDREN (KEY STAGE 2)**

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

1. ***I learn online*** – I use the school's internet, devices and logons for schoolwork, homework and other activities 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 if and when I am allowed to. If not sure, I will ask.
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 and 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 hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments, images or videos 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. If I make a mistake, I don't try to hide it but ask for help.
11. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about. I check with a trusted adult before I chat with anyone for the first time, even if they are a 'chatbot'.
12. ***I know new 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.
13. ***I never pretend to be someone else online*** - it can be upsetting or even dangerous.
14. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.

Acceptable Use Policy (AUP) for **CHILDREN (KEY STAGE 2)**

15. *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.
16. *I don't take photos or videos or people without them knowing or agreeing to it* – and I don't create artificial images, videos or deepfakes of others without consent. I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.
17. *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.
18. *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.
19. *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.
20. *I follow age rules* – 13+ games and apps 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 are very unsuitable.
21. *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.
22. *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).
23. *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.
24. *I am part of a community* – I do not say mean things, make fun of anyone or exclude them because they are different. If I see anyone doing this, I tell a trusted adult and/or report it. I talk to others online how I would like to be spoken to.
25. *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.
26. *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, know which sites to trust, and know how to double check information I find. If I am not sure, I ask a trusted adult.



SafeguardED

Acceptable Use Policy (AUP) for **CHILDREN (KEY STAGE 2)**

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 leave a message in my class 'I wish my teacher knew' box or get in touch with [Childline](#)

My Name: _____

Signed: _____

Date: _____

Acceptable Use Policy (AUP) for VISITORS AND CONTRACTORS

We ask all children and adults involved in the life of Sacred Heart Catholic Primary School 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 Designated Safeguarding Lead.

Further details of our approach to online safety can be found in the overall school [Online Safety Policy](#).

If you have any questions during your visit, you must ask the person accompanying you (if appropriate) and/or the School Office.

If questions arise after your visit, ask the School Business Manager by calling 020 89420215 or email school@sacredheart.merton.sch.uk.

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. The same principles apply for wearable technology. Smart glasses should not be worn in school. Please speak to the School Office if this presents any issue.
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 their contact details under any circumstances
 - I will protect (and not share) my username/password and notify the school of concerns.
 - I will abide by the terms of the school [Data Protection Policy](#) protections
 - I understand that my online activity will be subject to the school's filtering and monitoring systems,

Acceptable Use Policy (AUP) for VISITORS AND CONTRACTORS

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 (if by an adult).
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 any content or material which is or could be perceived to be inappropriate for children or an educational setting. I will not use a mobile hotspot to provide internet to any device I use in school.
10. If I need to use any specific applications, I must seek authorisation from the School Office before doing so. In particular this includes AI.
11. 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: _____

Acceptable Use Policy (AUP) for PUPILS WITH SEND

Acceptable Use Policy



What I Must do to Keep Safe Online and With Devices



Online means anything connected to the internet. Most devices and



apps are connected to the internet.



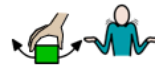
Devices are technology like: computers, laptops, games consoles,



tablets and smart phones.



I will only use the devices I am allowed to use.



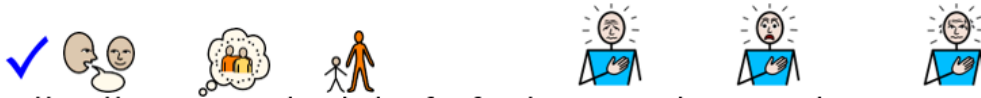
I will ask a trusted adult before I use new websites, games or apps.



I will ask for help if I'm stuck or not sure.



I will be kind and polite to everyone online.



I will tell a trusted adult if I feel worried, scared or nervous when I am using a device.



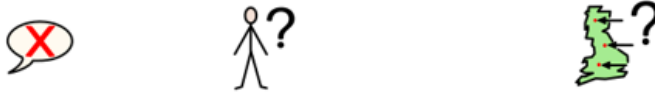
I will tell a trusted adult if I feel sad, angry or embarrassed when I am using a device.



I will tell a trusted adult if I feel bad or unsafe when I am using a device.



I know people online sometimes tell lies.



They might lie about who they are or where they live.



I never have to keep secrets from my trusted adults.



I will not change clothes or undress in front of any camera.



I will always ask a trusted adult before telling anyone my private



information or location.



I know that anything I do or say online might stay there forever.



It can be given to my family, my friends or strangers.



This could make me feel sad or embarrassed.



My trusted adults are _____ at school



My trusted adults are _____ at home



My name is _____