# ST FRANCIS OF ASSISI CATHOLIC PRIMARY SCHOOL
# ONLINE SAFETY POLICY

**Reviewed November 2025**
**Next review: September 2026**

**Contents**


| | |
|---|---|
| **1. Aims** | **2** |
| **2. Legislation and guidance** | **2** |
| **4. Educating pupils about online safety** | **6** |
| **5. Educating parents about online safety** | **7** |
| **6. Cyber-bullying** | **7** |
| **7. Acceptable use of the internet in school** | **9** |
| **8. Pupils using mobile devices in school** | **10** |
| **9. Staff using work devices outside school** | **10** |
| **10. How the school will respond to issues of misuse** | **11** |
| **11. Training** | **11** |
| **12. Monitoring arrangements** | **12** |
| **13. Links with other policies** | **12** |
| **Appendix 1: Acceptable Use Agreement (Families)** | **13** |
| **Appendix 2: Acceptable use policy (Staff)** | **16** |
| **Appendix 3: Acceptable use policy (visitors and contractors)** | **20** |
| **Appendix 4: Acceptable use policy (KS1)** | **23** |
| **Appendix 5: Acceptable use policy (KS2)** | **24** |
| **Appendix 6: online safety training needs – self audit for staff** | **27** |
| **Appendix 7: Acceptable use policy (SEND)** | **28** |
| **Appendix 8: Online safety incident report log** | **34** |

## 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

**The 4 key categories of risk**

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

## 3. Roles and responsibilities

### 3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Francesca Nelson-Smith

The governing board will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

### 3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

### 3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Undertaking annual risk assessments that consider and reflect the risks children face
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

### 3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

### 3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting any concerns of breaches directly to the DSL.
- Following the correct procedures by making a request in writing if they need to bypass the filtering and monitoring systems for educational purposes - giving reason for bypass and any risks associated with this.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

### 3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

## 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## 5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, the school's weekly newsletter and in information via our website or Google Classroom. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

## 6. Cyber-bullying

### 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

### 6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

### 6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher & DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

### 6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

St Francis of Assisi Catholic Primary School, recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

St Francis of Assisi Catholic Primary School will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

## 7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices

1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

## 8. Pupils using mobile devices in school

Pupils in years 5 and 6 may bring mobile devices into school, but are **not permitted to use them at any point of the day**. Mobile phones should be handed into the school office at the start of each day and will be returned at hometime.

The primary reason that year 5 and 6 students are allowed to bring a mobile phone to school is so that when walking home alone from school they are able to contact a family member in an emergency.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

## 9. Staff using work devices outside school

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 (e.g. asterisk or currency symbol)
- Ensuring their 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 locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3 and as set out in the staff code of conduct.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Head of School.

## 10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## 11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation (Prevent).

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

## 12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5. Reporting can also be done via CPOMS, staff should use the incident tag, online safety.

This policy will be reviewed every year by the school. At every review, the policy will be shared with the governing board.

## 13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy (AUP)

## Appendix 1: Acceptable Use Agreement (Families)

# Acceptable Use Policy (AUP) for Families

### Background

The use of technology is an essential part of all of our lives. At St Francis of Assisi 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 St Francis of Assisi Primary School 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 a copy of has been shared with families.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 St Francis of Assisi Primary School's full Online Safety Policy - here 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 the headteacher or DSL.

### What am I agreeing to?

1. I understand that St Francis of Assisi Catholic Primary School 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 understand that my child will have access to a google for education login. I will ensure that at home, they do not use anyone else's login information to submit work or comments to the teacher as another user.

7. I will support my child to follow the school's policy regarding bringing devices to school - Year 6 may bring a phone to school in case of emergencies when they are walking to and from school. I understand that the school would prefer for my child to not have a smartphone, but a basic mobile for making and receiving calls/texts. All phones must be turned off and handed to the office on arrival at school.
8. I understand that my child might be contacted online via google classroom, by their class teacher in regard to peninding pieces of work to be submitted and for feedback on their work.
9. 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.
10. 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.
11. 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 (for nearly every social media platform, this means under 13).
12. When I visit the school premises, I will keep any online technology in my pocket wherever possible.
13. I will follow the school's capturing digital images and video rules, 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 (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 via Arbor or google permissions.
14. 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 or DSL.
15. I understand that for my child to grow up safe online, they 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.

16. 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.
17. 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.
18. 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. 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
19. 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/
20. 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 - Pupil AUP and I understand that they will be subject to sanctions if they do not follow these rules.
21. I can find out more about online safety at St Francis of Assisi Primary School by reading the full Online Safety Policy here and can talk to the headteacher, DSL or class teacher, 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:** _____

## Appendix 2: Acceptable use policy (Staff)

# Acceptable Use Policy (AUP) for Staff

### Background

We ask everyone involved in the life of St Francis of Assisi 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 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 headteacher or DSL.

### What am I agreeing to?

I have read and understood St Francis of Assisi 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 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 identify.

4.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)

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. understand the sections on.

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'!

7.I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.

8.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).

9.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).

10.I will check with the headteacher if I want to use any new platform of app that has not already been approved by the school, to ensure this is quality assured.

11.I will follow best-practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods.

12.I will prepare and check all online sources and classroom resources before using them, for accuracy and appropriateness. I will flag any concerns about "overblocking" to the DSL.

13.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.

14.I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.

15.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.

16.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.

17.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.

18.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.

19.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.

20.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.

21.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.

22.I will not use any new technology or download any apps without agreement from the headteacher and Jartech Ltd.

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

24.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.

25.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.

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

27.I will only use gen AI platforms that have been authorised for use, and I will ensure that any use of these platforms is transparent, appropriate, legal and ethical. I will also ensure that I abide by all data protection legislation in relation to using these platforms.

28. I understand that when my employment is terminated with the school, the school may be required to access emails and my google drive account to maintain the effective running of the school.

**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 operations and HR Director or DSL**

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

**Systems:** **Google Workspace**
**Arbor**
**CPOMS**

**Additional permissions (e.g. admin)** _____

**Signature:** _____

**Name:** _____

**Role:** _____

**Date:** _____

## Appendix 3: Acceptable use policy (visitors and contractors)

# Acceptable Use Policy (AUP) for Visitors & Contractors

### Background

We ask all children, young people and adults involved in the life of St Franci of Assisi 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 DSL, Ailbhe Farrell, or the deputy DSL, Paula Murphy.

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 a senior member of staff. The following members of staff can be contacted:

Ailbhe Farrell
Paula Murphy
Colin Bartlett

If questions arise after your visit, send an email to the school office at office@franasssi.co.uk for the attention of the appropriate staff member.

### 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 (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, 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). Ailbhe Farrell is the DSL and headteacher.

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.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:** _____

## Appendix 4: Acceptable use policy (KS1)

# Acceptable Use Policy (AUP) for KS1 Children

My Name is _____

| | |
|---|---|
| To stay **SAFE online and on my devices**, I follow the Digital 5 A Day and: | |
| 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 or see 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, videos and photos. | |
| 11. I am **KIND** and polite to everyone. | |

My trusted adults are:

_____ at school.

_____ at home.

_____ at _____

Signature _____

## Appendix 5: Acceptable use policy (KS2)

# Acceptable Use Policy (AUP) for KS2 Children

**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 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 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 may be 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.

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 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.

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 can 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 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.

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:** _____

## Appendix 6: online safety training needs – self audit for staff

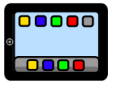
| ONLINE SAFETY TRAINING NEEDS AUDIT | |
|---|---|
| **Name of staff member/volunteer:** | **Date**: |
| **Question** | **Yes/No (add comments if necessary)** |
| Do you know the name of the person who has lead responsibility for online safety in school? | |
| Are you aware of the ways pupils can abuse their peers online? | |
| Do you know what you must do if a pupil approaches you with a concern or issue? | |
| Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors? | |
| Are you familiar with the school's acceptable use agreement for pupils and parents? | |
| Do you regularly change your password for accessing the school's ICT systems? | |
| Are you familiar with the school's approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? | |

# 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 _____

## Appendix 8: Online safety incident report log

| ONLINE SAFETY INCIDENT LOG | | | | |
|---|---|---|---|---|
| **Date** | **Where the incident took place** | **Description of the incident** | **Action taken** | **Name and signature of staff member recording the incident** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |