Online Safety Policy

Date Policy Created;	January 2023
Policy Created by;	L.Wordsworth/L.Clegg
Policy Agreed by Governors;	February 2023
To be reviewed;	Two years
UNCRC (United Nation Convention of the Rights of a Child) Articles included in this policy;	1, 2, 3, 4, 5, 6, 12, 15, 16, 17, 23, 24, 28, 34, 36 and 39

Our Mission Statement

Together we grow in faith, knowledge and love.

Together we show respect, kindness and confidence.

Together our community shines.

Our Mission Statement highlights the power of unity and shared values in fostering growth and positive relationships within a community. At St Anne's we work together with respect, kindness and confidence to truly make a difference. We aim to meet the needs of every child through a challenging, enriched curriculum. Providing a safe, secure and stimulating learning environment. We know when we come together our community thrives and shines

Development of the Policy

This policy will be reviewed annually, or more regularly in the light of any significant development in the use of the technologies, new threats to Online Safety or incidents that have taken place.
This policy applies to all members of the school community (including staff, pupils, governors, parents/carers, visitors and community users) who have access to and are users of the school's ICT systems, both in and out of school.

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, antisemitism, 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 scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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 signagree
account for its implementation. The governing board will co-ordinate 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 ● Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures ● Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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 Safeguarding Team and Computing Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions. The DSL works in collaboration with the DDSL's and Computing lead to take lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with ICT manager and all school based staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- 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 Technician – Remedian

The ICT technician 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 weekly 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 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, and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged 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
- 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
  National Online Safety

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.

3.8 Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreement.
- Should ensure that they follow the school's rules and procedures if they come across anything inappropriate or upsetting when using school ICT systems.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and incidents of cyber-bullying and know how to do so.
- Should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum and the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

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, workshops, in our weekly newsletter and through social media. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings when appropriate.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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 a member of the safeguarding team

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 1 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 will discuss cyber-bullying with their class in an age appropriate way. 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. The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher and senior leadership team must have permission from a parent or carer to 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 a member of the Safeguarding team. ● 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 cooperation

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 Safeguarding 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 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.

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. 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.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Playtimes or Lunchtimes
- Clubs before or after school, or any other activities organised by the school

All devices brought into school by pupils will be locked away in a secure cupboard during school hours. Pupil's place their device in an envelope with their name on for security. Pupils are asked to turn their phone off before handing their phone over. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement. 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 by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use. 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 ICT technician.

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 policies on behaviour and acceptable use.. 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 disciplinary procedures and 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.

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 up the risks
- 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 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. Online Safety Curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Online Safety program will be provided as part of Computing lessons – this will cover both the use of ICT and new technologies, both inside school and outside of school, and will be based on the

SMART internet rules developed by *Childnet* and resources from CEOP via the *thinkuknow* website.
● Key Online Safety messages should be embedded into other areas of the curriculum. ● Issues arising from reported Online Safety issues, including cyber-bullying, will be addressed in assemblies, with year groups or individual pupils as appropriate.
● Pupils should be taught in all lessons to be critically aware of the reliability of information found on the internet.
● Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside of school.
● Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
● Rules for use of ICT systems/internet will be posted in classrooms.
● Staff should act as good role models in their use of ICT, the internet and mobile devices.

13. Technical Information

The school will be responsible for ensuring that the school network (including associated hardware) is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. To allow for this to happen the following steps will be taken:

- The School ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements
- The school will use a Local Authority approved Internet Service Provider and filtering system. ●

All technologies will be risk-assessed with regard to Online Safety

- There will be regular reviews and audits of the safety and security of school ICT systems. ● Servers,

wireless systems and cabling must be securely located and physical access restricted.

- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the School Business Manager and will be reviewed, at least annually.
- All staff will be provided with a username and password that they must not divulge to others. Staff are responsible for ensuring passwords are updated where appropriate and remain secure.
- Pupils will be provided with a class username and password, which they must not share with other classes.
- The administrator passwords for the school ICT system, used by the ICT Technical Staff must also be available to the Headteacher and School Business Manager.

- In the event of the ICT Technical Staff (or another person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher and School Business Manager.

- Requests from staff for sites to be removed from the filtered list will be considered by the Online Safety Leader. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.

- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.

- An appropriate system is in place for users to report any actual / potential Online Safety incident to the Network Manager (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

In addition to the aforementioned steps, members of staff are responsible for ensuring the school's ICT infrastructure is not comprised by:

- Only ever using their individual username and password to access the school's network and logging off when they have finished their session.
- Always using Ctrl + Alt + Del and selecting 'lock' before leaving any school laptop unattended for any period of time.
- Only ever using hardware provided by the school with the school's ICT infrastructure. ● Never connecting school hardware to any personal device whether in school or at home. If documents completed on a personal computer are needed for work purposes they should be emailed to your school address and downloaded on site.

14. Staff Wireless Devices

The wireless devices (laptops, iPads, tablets, etc) provided by the school remain the property of the school at all times. As these items are entrusted to certain individuals an additional set of rules govern these items.

- Any member of staff who has been given a wireless device must adhere to the Acceptable Use Policy. ● The device must always be in school when the associated staff member is in school. ● The device may be taken off-site for work-related activities.
- The device may be connected to a **wireless** home network
- Personal USB based hardware (cameras, pen drives, external hard drives etc.) must not be connected to the device.
- The associated member of staff is responsible for the use of the device, at all times, while it is off-site. ● Personal files must not be stored on the device (this includes images and media files). ● Sensitive pupil or staff data must not be stored on any portable memory device. ● Permission from the Computing Leader must

be sought before installing any new software application. Updating existing applications is allowed.

- The device may be used for personal internet use (including forms of internet communication) providing that it does not contradict any of the rules set out in this Online Safety document or the Acceptable Use Policy.
- Any infringements of these rules, regardless of who has carried out the action, must be reported to the school's Online Safety Leader or the Headteacher as soon as possible.

15. Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

• When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

• Images should be stored on the school's network with access limited to school staff. • Digital images must be uploaded and deleted from media cards at the first opportunity. • Staff are allowed to take digital / video images to support learning, but must follow school policies concerning the sharing, distribution and publication of those images. Images should only be recorded using school equipment and never on personal equipment.

• Members of staff must be able to justify the reasons behind taking and storing any digital media file (including image and sound).

• Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. • Pupils must not share, publish or distribute images of others.

• Written permission from parents or carers will be obtained in compliance with GDPR 2018 before photographs can be taken, used within school, or published on internet-based platforms. Text that accompanied such images will not name any child. For example – 'year five pupils enjoying a music lesson.'

• An up-to-date list of photograph permissions is kept in the office and on the server it is the responsibility of the person recording the images to check the list.

16. The School's Website (https://www.stannescrumpsall.co.uk/)

St Anne's RC Primary School uses its website to celebrate successes, share information and keep parents / carers informed about events taking place. Furthermore, the school's website also provides information about the school's curriculum and performance data.

17. The Use of YouTube

The school has unblocked the video-sharing site you-tube to allow teachers and pupils to benefit from the rich variety of educational content that it offers. However, as the site is also used to share videos socially the following rules must be adhered to, to help ensure the safety of the pupils and the integrity of the school's network:

● All staff must read the Acceptable Use Policy before accessing YouTube in school in any capacity. ● Staff have access to YouTube to support teaching and learning, personal use of YouTube is allowed outside of directed hours, so long as this is in compliance with the Acceptable Use Policy. ● Teachers must not search for videos in front of the class; all videos must be found prior to the lesson. ● As YouTube videos do not come with age classification advice, teachers must watch the entire video to assess the suitability of the resource for the pupils they teach.

- Teachers must be aware that YouTube is a commercial site and that videos may contain adverts. If adverts are displayed as part of the video it is suggested that the commercial nature of the site is discussed with the class.
- Pupils are not allowed to use YouTube on their individual devices; any videos that they need to be watched to support their learning, should be shown to the entire class through the room's interactive whiteboard.
- If an inappropriate video / image is displayed, the screen should be turned off and the incident reported to the Headteacher or Computing Leader as soon as possible.

18. The Use of Social Media

The school uses Twitter, Instagram and Facebook as an additional tool to promote parental engagement by sharing photos and information about events, activities and success of the pupils. Examples are; pictures of artwork completed by the class; pictures of classroom displays; pictures of children on class trips, curriculum events etc. To ensure the staff use of Twitter, Instagram and Facebook is consistent with the rules already laid out within the policy they must adhere to the rules below.

- All staff must read the Acceptable Use Policy before accessing any social media platforms in school in any capacity.
- Any staff member who wishes to use one of the social media platforms will post on the St Anne's account. This account must only be used in a professional context.
- An image of the school's badge is to be used as a profile picture.
- Personal twitter accounts must not be linked to school twitter accounts.
- Images, including those of pupils, can be tweeted but must adhere to the digital images section of the school's Online Safety policy.
- Staff are responsible for checking the content and the appropriateness of any websites they post links to. ● Staff must be aware that all messages / tweets can be seen by anyone accessing the web platform.

19. Communications

A wide range of rapidly developing communications technologies have the potential to enhance learning. This section details the technologies the school currently allows the use of and the manner in which they should be

used.

- All staff will be provided with a school email address, which is to be used solely for communication regarding their job. Users need to be aware that email communications may be monitored. You should only use your email address to register to website that are of an educational basis and not for personal social media sites.
- The school regularly communicates with the staff through email, it is therefore expected that staff check their email daily.
- Staff may access personal emails within school outside of directed hours, so long as this use complies with the school's Acceptable Use Policy.
- Attachments emails should only be opened if they are from known sources and never on personal email.
- Children are prohibited from using mobile phones within school although the school will allow pupils to bring a mobile phone to school, which needs to be left in the school office. If parents / carers wish their children to bring a mobile phone to school, they must inform the school in writing and understand that the school accepts no responsibility for any damage that may occur to these phones while in the school's possession.
- All users must immediately report, to the Online Safety Leader, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Parents who wish to communicate (usually this is complaints, compliments or questions) to the school or teachers by email should do so via the admin@ account and request for the attention of the Class Teacher rather than using personal emails. This is to protect staff wellbeing and ensure clarity in communication.
- Staff should be aware that under the freedom of information act all emails are subject to disclosure (to any party) and can be used in a court of law if required.
- Any digital communication between staff and pupils must be professional in tone and content. These communications may only take place on official (monitored) school web applications and messages **should not be private**. The use of any other form of digital communication (including personal accounts) is strictly prohibited.
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website.

20. Staff Use of Mobile Phones

Although mobile phones are an essential personal communication tool, they also provide a distraction for both staff and pupils. To minimise the disruption to learning all teaching staff (teachers, teaching assistants) need to follow the below rules. Mobile phones should be switched off or to silent and placed out of sight during teaching times, regardless if you are working with pupils or preparing resources. Personal phone calls should only be made before

school, at break and lunchtimes, or after school and should take place in the staffroom or an empty classroom. **No** member of staff should be walking around school using their mobile phone. While the use of the mobile internet network is allowed, staff must only access websites, and website based apps (facebook), that are consist with the rules set out in this document and the Acceptable Use Policy.

21. Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. Users shall not visit Internet sites, make posts, download, upload, data transfer, communicate or pass on, materials, remarks, proposals or comments containing or relating to:

- Child sex abuse images
- Promotion or conduct of illegal acts
- Adult material that potentially breaches the Obscene Publications Act in the UK • Criminal racist material in the UK
- Terrorists or extremist groups
- Pornography
- Promotion of any kind of discrimination
- Threatening behaviour, including the promotion of physical violence or mental harm • Any other information that may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Running a private business
- Systems, applications, websites or other mechanisms that by pass the filtering or other safeguarding employed by the local authority or the school
- Uploading or downloading or transmitting commercial software or any copyrighted materials belonging to third party, without necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Personal social network sites
- Carrying out sustained or instantaneous high-volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- Gambling sites
- File sharing

This list must be adhered to regardless of the device used to connect to the internet.

22. Monitoring and reporting

In accordance with Manchester Safeguarding Children's Board policy the school will maintain an incident log (on CPOMs) of Online Safety incidents, including cyber-bullying that include:

- A description of the event
- Details of people involved
- How the incident was identified
- What actions were taken
- Conclusion of the incident

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Respectful Relationships and Behaviour Management policy (behaviour policy) ● Staff disciplinary procedures and policies
- Data protection policy and privacy notices
- Complaints procedure

Staff Agreement

I understand that I am responsible for my actions in and out of school:

•I understand that the Online Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

•I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the St Anne's RC Primary School's Online Policy and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff Name

Signed

Date