St Jude's Church of England Primary School

Online Safety Policy

Our children

Our St Jude's family

Happy – Inspired – Loved

The sky is not the limit

Ready for today - prepared for tomorrow

Scope of the Online Safety Policy

This policy applies to all members of the St Jude's community (including staff, students / children, volunteers, parents / carers, visitors, community users) who have access to and are users of our ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of children when they are off the school site. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate Online Safety behaviour that take place out of school.

The Role of the Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor.

The role of the Online Safety Governor will include:

- termly meetings with the Online Safety Leader
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meetings

The Role of the Headteacher

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Leader.

The Headteacher and Deputy Headteacher will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff **(see Appendix 1).**

The Headteacher is responsible for ensuring that the Online Safety Leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the Online Safety Leader.

The Role of the Online Safety Lead

The Online Safety Lead:

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments **(see Appendix 2)**
- meets termly with the Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team

The Role of the Network Manager

It is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. The managed service provider is fully aware of the school Online Safety Policy and procedures.

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher and Online Safety Leader for investigation
- that monitoring software / systems are implemented and updated as agreed in school policies

The Role of the Teaching and Support Staff

The teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher and Online Safety Leader for investigation

- all digital communications with children, parents and carers should be on a professional level and only carried out using official school systems
- children understand and follow the Online Safety Policy and acceptable use policies
- children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

The Role of the Designated Safeguarding Leads

The Designated Safeguarding Leads should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

(n.b. it is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop).

The Online Safety Group

The Online Safety Group provides a consultative service that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

The group will also be responsible for regular reporting to the Governing Body. Members of the Online Safety Group will assist the Online Safety Leader with:

- the review and monitoring of the school Online Safety Policy
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring incident logs
- consulting stakeholders – including parents, carers and children about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool

The Role of our Children

Our children:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement **(see Appendices 3 and 4)**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the use of images and on cyber-bullying
- 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, if related to their membership of the school

The Role of our Parents and Carers

Our parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website Online Safety section and Online Safety parent workshops.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and interaction with the school through twitter and Google Reviews
- their children's personal devices in the school

The Role of Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school academy systems **(see Appendix 5).**

Education in Online Safety

Education for our children

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in online safety is therefore an essential part of the school's online safety provision.

Children and young people 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 curriculum should be provided as part of Computing lessons and should be regularly revisited
- Key online safety messages should be reinforced throughout the year on the school website and in the newsletter
- Children should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Children should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Children should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students / children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education for our Parents and Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours.

Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Online Safety Newsflashes
- Parent workshops
- Online Safety Week and safer Internet Day

Education for our Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups to enhance their Online Safety provision

Education and Training for our Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out annually.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator Leader will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in during our Spring INSET day.
- The Online Safety Leader will provide guidance and training to individuals as required.

Education and Training for our Governors

Governors should take part in online safety training sessions, with particular importance for those who are members of any subcommittee involved in technology, online safety and safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority

- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies and lessons).

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes

- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents

Staff will ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

St Jude's Online Safety Mission Statement

(see Appendix 6)

In this day and age, online safety has to be more than a reminder not to speak to strangers online. As children begin to navigate the internet and use it in different ways as they grow older, their own personal conduct online is also an area where they need guidance. We believe it is important to teach children both about the technological and social and emotional aspects of being safe and successful online.

At St Jude's C of E Primary School, we want staff, children, parents and carers to create a school community that embraces the use of different technologies to enhance learning and thinking, as well as teach all of our children how to be safe and responsible digital citizens, who make informed decisions about their actions online. We believe that the internet is a great resource and tool.

Policy History

	Date	Lead
Date drafted	9th December 2017	David Winn (Online Safety Leader)
Date refined		
Date agreed		
Date published		
Review date		

This policy was adopted by the full Governing Body of St Jude's CE Primary on

_____ and supersedes all previous policies to date.

Signed: _____

(Chair of the Pupil & Curriculum Committee)

Signed: _____ (Chair of Governors)

Date: _____

Appendices

1. Responding to incidents of misuse – flow chart

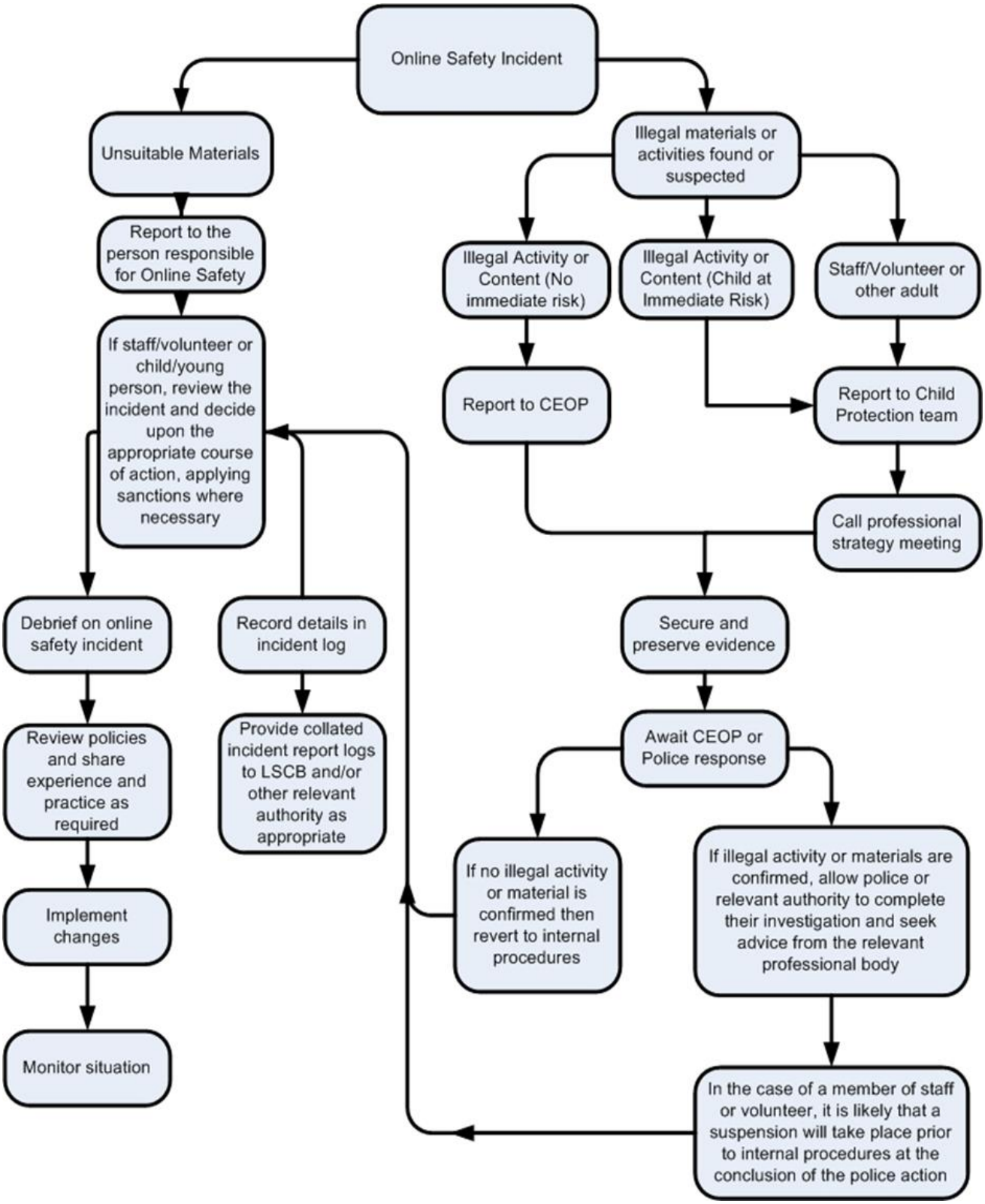
2. Incident Reporting Log

3. Pupil Acceptable Use Agreement – EYFS & KS1

4. Pupil Acceptable Use Agreement – KS2

5. Community User Acceptable Use Agreement

Appendix 1


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Appendix 2

Reporting Log Group:						
Date	**Time**	**Incident**	**Action Taken**		**Incident Reported By**	**Signature**
			What?	**By Whom?**		

Appendix 3

Pupil Acceptable Use Policy Agreement (EYFS & KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): .....

Signed (parent): .....

Date: .....

Appendix 4

Pupil Acceptable Use Policy Agreement (KS2)

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include (schools / academies should amend this section to provide relevant sanctions as per their behaviour policies) loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing the school website or discussing the school in any way via social media or online platforms.

Name of Pupil: .....

Class: .....

Signed: .....

Date: .....

Appendix 5

Community Users Acceptable Use Policy Agreement

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems

I have read and understand the above and agree to use the school digital technology 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.

Name: .....

Signed: .....

Date: .....

St. Jude's Church of England Primary School

Online Safety Mission Statement

At St Jude's C of E Primary School, we want staff, children, parents and carers to create a school community that embraces the use of different technologies to enhance learning and thinking, as well as teach all of our children how to be safe and responsible digital citizens, who make informed decisions about their actions online . We believe that the internet is a great resource and tool.

At home, many children also use computers and mobile devices to play games, learn and explore. Make talking about what they're up to online a normal part of everyday life, rather than something that only happens when there's a problem or issue. We believe regular, open conversations between parents, carers and children about using the internet is ultimately the best way to keep children safe online.

While there are huge benefits to being online, it is important to be aware that any time children use the internet they do face some potential risks, ranging from accessing inappropriate or harmful content, oversharing their own personal information and online bullying. We believe understanding what your child is doing online helps keep them safe online.

There are some websites and games that have age restrictions and checks on them to make sure that children don't see unsuitable content. The same goes for social media networks. It is our expectation that children at St Jude's do not have their own social media accounts. This is because children must be at least 13 to register on most social networking websites. However, the reality is there's not a lot standing in the way of children joining at a younger age so it is vital as parents and carers that you really take an interest in your child's online behaviour and have a good overview of how they use their computer or mobile device to ensure they are only accessing content that is appropriate for their age. We believe age restrictions are there for a good reason.

In this day and age, online safety has to be more than a reminder not to speak to strangers online. As children begin to navigate the internet and use it in different ways as they grow older, their own personal conduct online is also an area where they need guidance. We believe it is important to teach children both about the technological and social and emotional aspects of being safe and successful online.