E-Safety Policy

St Jude's CE Primary School exists to serve its community by providing education of the highest quality within a Christian framework of values and beliefs.

We help children to achieve their full potential by fostering a sense of belonging, encouraging their determination, faith, respect and love for each other, and teaching the importance of being honest, selfless and thankful.

WHAT DOES E-SAFETY INCLUDE?

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Common technologies include:

- the Internet;
- email;
- instant messaging
- blogs / Twitter;
- podcasts;
- social networking sites such as Facebook;
- location based social networking such as Google Latitude;
- video broadcasting sites such as YouTube;
- chat rooms, where still used;
- Skype;
- online gaming rooms and platforms;
- music download sites;
- mobile phones with camera and video functionality
- and applications

HOW DOES INTERNET USE BENEFIT EDUCATION?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of
- networks and automatic system updates;
- and exchange of curriculum and administration data with the Local Authority and DfE; access to learning wherever and whenever convenient.

MANAGING E-SAFETY AT ST JUDE'S

1. Education

- ensure pupils are supervised when using ICT resources as far as is reasonable;
- teach pupils to know and understand the rules of appropriate use;
- regularly provide e-safety advice for pupils, staff and parents e.g. workshops, newsletters, assemblies and via the website;

- teach pupils about the risks of the commercial use of the internet e.g. online gaming and buying online;
- advise to STOP and THINK before they CLICK;
- ensure children are aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- ensure [for older pupils] understand how search engines work and to understand that this affects the results they see at the top of the listings;
- explain why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- explain why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- explain why they must not post pictures or videos of others without their permission;
- advise not to download any files – such as music files - without permission;
- have strategies for dealing with receipt of inappropriate materials;
- and explain [for older pupils] why and how some people will 'groom' young people for sexual reasons.

2. Internet

- ensure pupils only publish within the appropriately secure school's learning environment;
- preview websites before use to ensure they are appropriate
- and are vigilant when conducting 'raw' image searches

3. Mobile phones

- children are not allowed to bring mobile phones to school unless a written request has been submitted to the head teacher and permission has been granted and this is only granted in exceptional circumstances
- and use of mobile phones is restricted within the building and is to be avoided within the playground for staff/parents and visitors. Use is restricted to the admin area only NOT the entrance hall.

4. Social Networking

- only permit pupils to use video conferencing and other social networking sites, e.g. Manga High, as a planned curriculum project.

5. Cyber-bullying

- treat cyber-bullying as bullying. Please see Anti-Bullying policy;
- ensure pupils and staff know what to do if there is a cyber-bullying incident
- and ensure that instances of cyber-bullying will be reported in line with existing anti-bullying policies and procedures in schools. The victims of cyber-bullying will be reassured they have done the right thing in disclosing the bullying and be supported. For further information, please see section – additional online advice and support on page 4.

6. Security

- ensure all staff and pupils have signed an acceptable user agreement form and understand that they must report any concern and keep a record of this on file;
- ensure parents provide consent for pupils to use the internet
- and work in partnership with the Local Authority, Becta and the Internet Service Provider to ensure filtering systems are as effective as possible

7. Staff

- inform staff and pupils that they must report any failure of the filtering systems directly to Admin Assistant
- and ensure staff know how to send or receive personal and sensitive data and understand the requirement to encrypt data where the sensitivity requires data protection

8. Filtering

- work in partnership with the Local Authority, Becta and the Internet Service Provider to ensure filtering systems are as effective as possible.

9. Video Conferencing

- ensure pupils are only ever permitted to use video conferencing as part of a planned curriculum project with permission given by the supervising teacher.
- and videoconferencing will be appropriately supervised for the pupils' age.

10. Data Protection

Please refer to the school's Data Protection Policy

FREQUENTLY ASKED QUESTIONS AND ANSWERS

Q1 Should I use my personal mobile phone or camera to photograph or video children / young people I work with?

A No. Any photographic or video images of children / young people should always be recorded and stored on equipment belonging to the organisation after written consent from the parent/carer and with the agreement of the child/young person and the organisations senior management. Care must be taken to ensure that images are stored appropriately and securely.

If at any time you are witness to visible injuries or other signs of abuse or neglect (i.e. bruising or scarring), you must not under any circumstances take any photographic images of this. Only medical staff and the Police Child Abuse Investigation Team (CAIT) are permitted to take photographic evidence.

Q2 How can I store personal data safely?

A Electronic personal and confidential information must always be kept secure on hard drives or memory sticks but must be password protected and encrypted in line with the school's Acceptable Use of Internet & Data Protection policies.

ADDITIONAL ONLINE ADVICE & SUPPORT

www.lambethscb.org.uk	Lambeth Safeguarding Children's Board
www.ceop.police.uk	Child Exploitation Online Protection Centre for reporting internet abuse
www.thinkyouknow.co.uk	Practical online advice and training resource for children, parents and teachers.
www.clickcleverclicksafe.direct.gov.uk	Internet safety advice from the UK Council for Child Internet Safety
www.digizen.org/cyberbullying	Department of Education and Childnet advice and guidance on cyber-bullying

The school's e-safety policy will operate in conjunction with other policies including those for Data Protection and Security. The school will appoint an e-Safety coordinator. In many cases this will be the ICT / Designated Child Protection Officer as the roles overlap.

This policy is a working document and will be reviewed every year.

Last reviewed: May 2013

Appendix 1

E-Safety Audit

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with LA guidance?	
Date of latest update: April 2013	
The Policy was agreed by governors on: May/ 2013	
The Policy is available for staff at: School network and School website	
And for parents at: school office and school website	
The designated Child Protection Coordinator is: Ms Florence Wilson	
The ICT / e-Safety Coordinator is: Ms Monique Darrell	
Has e-safety training been provided for both pupils and staff?	
Do all staff sign an ICT Code of Conduct on appointment?	
Have school e-Safety Rules been set for pupils?	
Are these Rules displayed in all rooms with computers?	
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access.	
Has the school filtering policy been approved by SMT?	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	

Appendix 2

E-safety advice to parents / carers

Those with parental responsibility for children should pay particular attention to the following 'rule of thumb' advice in order to safeguard young people they hold parental (including temporary) responsibility for.

Please remember that most children / young people have internet access via their own mobile phones, laptops and tablet computers which can be restricted by using the relevant parental consent controls (foster carers should always verify what restrictions they can impose directly with the young persons allocated social worker) and via certain online gaming platforms such as X Box and Playstation.
Parents / carers and foster carers of children with additional needs or vulnerabilities must appreciate that their children will require additional support around e-safety, particularly if their child is:

- disabled;
- has special educational needs or learning difficulties;
- is looked after and placed in an area unfamiliar to them;
- is out of mainstream education;
- speaks English as a second language (or does not understand English);
- known to have gang associations;
- has been the victim of bullying or crime or has lived with domestic violence;
- is gay or unsure about their sexuality;
- has emotional or learning difficulties or does not fully understand the impact; of their actions;
- has been the victim of bullying
- and has inconsistent access to education (i.e. is a traveller).

Parents / carers and foster carers should take advantage of the many online resources available via the parents section of the ThinkYouKnow website www.thinkyouknow.co.uk

It is also recommended that they download the Child Exploitation Online Protection tool onto all computer browsers www.ceop.police.uk .This tool provides instant online access for reporting any form of online abuse.
They should also encourage children to download this tool directly onto their Facebook or other social network profile page which will act as a deterrent to potential perpetrators.

Restricting access to unsuitable websites

The following websites are examples of those which pose threats to or may be unsuitable for young people and access may have to be restricted or denied by using appropriate filters

- those which are sexually explicit or contain information of a sexual nature;
- those which permit the purchase of or promote the usage of drugs, alcohol or tobacco;
- personal and dating websites;
- age inappropriate chat rooms and social networking sites;
- certain gaming platforms and websites via X Box, Playstation, Wii etc;
- websites promoting eating disorders;
- websites promoting suicide
- and websites which teach criminal activities or skills including the purchasing, or enabling, of weapons and which advocate terrorism or extremism.

Key Stage 1 e- Safety rules

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Appendix 4

Key Stage 2

Think then Click

e-Safety rules for Key Stage 2

- We ask permission before using the Internet.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- All of our electronic communications (email, tweets, blog comments) are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Appendix 5

PUPIL INTERNET USER AGREEMENT

St. Jude's Internet system has been provided to meet the needs of pupils and staff, by enhancing and improving their education. It is available for staff to use for professional development, teaching, research, administration and management. This Internet policy has been created to protect all users of the school's system.

The school reserves the right to examine and delete any files held on the computer system. It also holds all rights to monitor visited internet sites, this will be done on a regular basis.

All members of staff are responsible for ensuring that pupils adhere to the following stated procedures:

1. Access must ONLY be made via the authorised account and password, which must NOT be made available to any other person;

2. The use of the internet should be appropriate to the student's education and to staff professional development;

3. Any activity that threatens the integrity of the school's ICT systems, or attack;

4. Visited sites and accessed materials must be appropriate to work in school. Users will recognise inappropriate materials and should expect to have their access removed if these materials are accessed;

5. Users are responsible for e-mails they send and for contacts that may result in e-mails that may be received;

6. Professional levels of language and content must be applied as for letters or other media, as e-mails are often forwarded and can be inadvertently sent to the wrong person;

7. Posting anonymous messages and forwarding chain letters is forbidden;

8. Copyright and intellectual property rights of materials must be respected;

9. Legitimate private interests may be followed, providing School use is not compromised;

10. Use for financial gain, gambling, political purposes or advertising is forbidden.

11. The use of the school's internet system to access inappropriate materials such as pornographic, racist or any offensive materials is strictly forbidden.

12. Pupils may not transport disks to and from school.

Staff requesting access must sign to agree this policy.

Signed……Date……

PRINT NAME ……

Appendix 6

STAFF ICT USER AGREEMENT

Computers, associated hardware, software and internet access have been provided by St Jude's School to help staff and pupils work or study in a more effective way. The equipment and internet are available to staff to use for professional development, teaching, researching, administration and management. These policy guidelines have been created to protect all users of the school's system.

Staff laptops (or similar) may be used by staff at home by written agreement with the headteacher.

The school reserves the right to examine and delete any files held on the computer system. It also holds all rights to monitor visited Internet sites; this will be done on a regular basis.

Staff must not use school computers for any form of illegal activity, e.g. downloading copyright material, introducing virus', hacking into other computers, viewing or downloading pornographic, obscene, offensive or any other inappropriate material from any source; transmitting or storing such material on a school computer.

Action you must take if you inadvertently access inappropriate material

Anyone inadvertently accessing inappropriate material should immediately inform the Head teacher or designated person in school and ensure that the incident is recorded in the eSafety incident log.

All members of staff must agree to the following procedures:

COMPUTER USE

1. I will only access the computer system via my account and password, which I will not make available to any other person.

2. I will take all reasonable steps to ensure that all laptops and memory devices are fully virus protected and that protection is kept up to date.

3. I will report any accidental access to material which might be considered unacceptable immediately to my line manager and ensure it is recorded.

4. Confidential school information, pupil information or data which I use will only be stored on a device which is encrypted or protected with a strong password. Computers will have a password protected screensaver and will be fully logged off or the screen locked before being left unattended.

5. I understand that I have the same obligation to protect school data when working on a computer outside school.

6. I will report immediately any accidental loss of confidential information so that appropriate action can be taken.

INTERNET USE

1. During school hours, I will only use the computers and the internet for work related activities. I understand that reasonable personal use is permitted outside recorded working time e.g. at lunchtime.

2. Visited sites and accessed materials will be appropriate to work in school. If I receive/see inappropriate materials I will not access them and alert the ICT Coordinator if necessary.

3. I will always use professional language and content in emails I send or forward.

4. I will not send anonymous messages or forward chain letters.

5. To protect my own privacy I will use a school email address and school telephone numbers (including school mobile phone) as contact details for pupils and their parents.

6. I know that emails are governed by the same rules which cover all home-school correspondence. Therefore, I will save electronic copies, and keep in the Shared Staff Area.

7. If I use instant messaging, chat rooms, webcams or forums for communicating with pupils or parents it will only be via the school's accredited system or Virtual Learning Environment (VLE).

8. I will not share personal details or have online friendships with parents or pupils, except in special circumstances i.e. such pupils are also related to me.

9. I know that any comments made on social networking sites relating to the school or pupils in the school may be misinterpreted and could result in disciplinary action.

10. I will only use real time communication e.g. web cams for educational purposes.

11. I will inform the ICT Coordinator, Deputy or Headteacher if I suspect or witness misuse of the Internet and Computer systems by pupils, staff, or visitors.

12. If I receive inappropriate material I will immediately inform the ICT Coordinator/Management.

13. If I receive inappropriate and offensive material from staff/parents/pupils, I will immediately save a copy, print a copy, and inform the Headteacher.

I understand that the school may monitor or check my use of ICT equipment and electronic communications.

I understand that by not following these rules I may be subject to the School's disciplinary procedures.

Name*……..*

Signed*…….*

Date*……*

Appendix 7

Consent Form for Photography and Images of Children

During your child's life at St Jude's School we may wish to take photographs of activities that involve your child. The photographs may be used for displays, publications such as our school prospectus, recordings (videos/DVDs) of school productions, events, our website and for local newspapers. Photographs and recordings are also used within school as part of the assessment of children's learning.

Photography or filming by agencies external to the school will only take place with the permission of the Headteacher and under appropriate supervision. Should we wish to use an image of your child on our website or in a school publication, we will contact you to receive our express permission. When filming or photography is carried out by the news media, children will only be named if there is a particular reason to do so (eg they have won a prize), and home addresses will never be given out.

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child for promotional purposes. Please answer the questions below, sign and date the form and return it to us as soon as possible. You can ask to see the images of your child held by us and you may withdraw your consent at any time

<table>
<tr><td colspan="3">Name of child (block capitals) Class:</td></tr>
<tr><td colspan="3">Name of person responsible for the child:</td></tr>
<tr><td colspan="3">I understand that :
• staff, pupil or professional photographers acting on behalf of the school may take images for use in displays, ceremonies, presentations or on the school website;
• the local media may take images of activities that show St Jude's School in a positive light eg drama, musical performances, prize giving etc;
• embarrassing or distressing images will not be used;
• the images will not be associated with distressing or sensitive issues;
• the school will regularly review and delete unwanted material.</td></tr>
<tr><td rowspan="2">Having read the above statement, do you give your consent for photographs and other images to be taken and used?
(please tick the appropriate box)</td><td></td><td>YES
I give my consent for pictures to be taken and used</td></tr>
<tr><td></td><td>NO
I do not give my permission for pictures to be taken and used</td></tr>
<tr><td colspan="3">Signature of person responsible for the child:</td></tr>
<tr><td colspan="3">Relationship to the child:</td></tr>
<tr><td colspan="3">Date: (day/month/year)</td></tr>
</table>

Please note that there may be other circumstances falling outside the normal day to day activities of the school in which pictures of the children are requested. We recognise that in such circumstances specific consent from the parent/guardian will be required before photography or filming can be permitted.

If you wish to attend school functions and take photographs of your and other people's children, please take appropriate images. Be sensitive to other people and try not to interrupt or disrupt concerts, performances and events. Please note that on some school occasions, photography may not be allowed.

PLEASE RETURN THE FORM TO THE SCHOOL OFFICE