ST JAMES' RC E-SAFETY POLICY

Faith in action,

Growing together,

Walking in the footsteps of Christ.

Development of this Policy

This e-safety policy has been developed by the e- Safety Subject Leader, the staff and SLT.Consultation with the whole school community has taken place through a range of formal and informal meetings.
It has been approved by the Governors.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governors on:	
The implementation of this e-safety policy will be monitored by the:	E-Safety Subject Leader
Monitoring will take place at regular intervals:	Every 2 years
The Governors will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Every term
Should serious e-safety incidents take place, the following people should be informed:	E-Safety Subject Leader, CPO,

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited in planning)
- Surveys / questionnaires of ppupils, parentsand staff.

Roles and Responsibilities:

The Head teacher, E-Safety Subject Leader and Governors will ensure that:

- The policy is reviewed bianually or whenever need arises
- Appropriate response is given to any e-safety incident
- Overall management of e-safety with in school.
- Keeping up to date with emerging risks and threats through technology use
- E-safety is observed in all aspects of technology within school (ICT suite, laptops, ipads, cameras.)
- That there is a communal e-safety log that records any incidents.

Pupils will ensure that:

- They are responsible for using the all-digital technology systems in accordance with the pupil Acceptable Use Policy
- They have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Year 6 will be expected to know and understand policies on the use of mobile devices.
- They should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the e-Safety Policy is applicable wherever they are using technology.

All Parents / Carers will ensure that:

They support the school in promoting good e-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.

The school will take every opportunity to help parents understand these issues through curriculum evenings, newsletters, letters, website and information about national / local e-safety campaigns.

Network Manager:

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 e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply.
- that users may only access the networks and devices through properly enforced password protection, in which passwords are regularly changed.
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- that the use of the network/internet is regularly monitored in order that any misuse/attempted misuse can be reported to the Head teacher/ E-Safety Coordinator/Designated Senior Leader for investigation/action.
- that monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Agreement .
- they report any suspected misuse or problem to the Head teacher/E-Safety Subject Leader.

- all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems, checked by the Head teacher.
- e-safety issues are embedded in all aspects of the curriculum and other activities.
- students understand and follow the e-safety and acceptable use agreements.
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, ipads, laptops, computers, 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 students 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

Designated Safeguarding Lead:

The designated safeguardinglead should be trained in e-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

Teaching and Learning

Why interent use is so important.

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience. Internet use is a part of the statuatory curcculum and a necessary tool for staff and pupils. It enables schools to communicate with other school internationally and to share good practice.

Internet use will enhance learning.

The school internet acces is designed expressly for pupil use and includes filtering approparriate to the age of pupils. Pupils will be taught what internet use is accetable and what is not and be given clear objectives for internet use. Pupils will be educated in the effective use of the internet in reasearch, including the skills of knowledge locataion, retreival and evaluation.

Pupils will be taught how to evaluate internet content.

The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read an shown how to validate infomration before accepting its accuracy.

Bring Your Own Device (BYOD):

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD. Use of BYOD should not introduce vulnerabilities into existing secure environments. Please see the Mobile Phone Policy for further details.

Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. The school has a strict policy of Year 6 student's phones having no access to the internet.

- The school has a set of clear expectations and responsibilities for all users.
- The school adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement.
- All network systems are secure and access for users is differentiated.
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.
- Students receive training and guidance on the use of personal devices.
- Regular audits and monitoring of usage will take place to ensure compliance.
- Any device loss, theft, change of ownership of the device will be reported.

Use of digital and video images:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students 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.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, as a school we encourage and instruct parents that these images should not be published/made publicly available on social

networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.

- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website through the Acceptable Use Contracts.
- Student's work can only be published with the permission of the student and parents or carers.

Social Media - Protecting Professional Identity:

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk. School staff should ensure that:
- No reference should be made in social media to students, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for **professional** purposes will be checked regularly.

Twitter Guidelines

The school is using Twitter to raise our social profile in the community and to interact and inform parents of current events. To ensure online safety:

- The Head Teacher is the only person who posts through the twitter handle.
- No photos or information that could identify a child (ie. Ones of their faces/names) will be included on the Twitter updates.
- The school will follow only educational users and not retweet any other tweets.

In the Event of Inappropriate Use

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur:

- If children accidentally access something inappropriate on the internet, the children know to immediately close the laptop or turn off the monitor of the desktop computer. They know to immediately tell a teacher. Where appropriate, parents will be contacted to advise them.
- All incidents will be recorded in the E Safety Incident log book, checked regularly by LMT and the E Safety Subject Leader.
- Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home or a phone call to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time.
- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult
- The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.
- Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Responding to incidents of misuse:

This guidance is intended for use when staffs need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities; in this case the Head Teacher will phone the police.

Secure transfer of data and access out of school

St James' School recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies.

In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software;
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe.

Further Data Protection will be in place following the update of the ICT suite and the GDPR.

Monitoring and Evaluation

This policy will be updated in line with any new developments in the school and/or any new government guidance. All staff are expected to follow the policy and the Leadership Team, following ongoing regular reviews of classroom practice, will be responsible for ensuring the effectiveness of practice across the school.

This Policy will be renewed annually.

It was last reviewed in: December 2017

It will next be reviewed in: December 2018

This statement of policy was approved by the Governing Body at their meeting on:-

Date: _______________________________________

Signed: ____________________________ (Chairperson)

_____________________________________ (Head teacher)

APPENDIX 1 ACCEPTABLE USE POLICY

St James' RC Primary SchoolAcceptable Use Policy for Internet Access

As part of the school's continuing ICT development, we offer pupils of St. James' RC Primary School access to facilities that include the Internet. Before being allowed to use the Internet, it is a statutory requirement that all pupils must obtain parental permission and both they and you must sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on this matter.

Access to the Internet will enable pupils to explore thousands of websites throughout the world – an important interaction in this digital age. LGFL (London Grid for Learning) provides a filtered and secure intranet and provides us with a strict and secure Firewall but the nature of the Internet is such that sites which contain these sorts of materials are constantly changing which means that no filtering can be perfect. Whilst our aim for Internet use is to further education goals and objectives, pupils may find ways to access other material as well.

We believe that the benefits to pupils from access to the Internet exceed any disadvantages, although ultimately, parents and guardians of pupils are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end this school supports and respects each family's right to decide whether or not to allow their child access.

Staff will provide guidance to pupils so that they will be able to manage risks when they make use of telecommunications and electronic information sources to conduct research and other studies related to the curriculum. A member of staff will supervise pupils while they are using the Internet or email.

As much as possible, pupils will be directed to information resources that have been reviewed and evaluated prior to use. While pupils may be able to move beyond those resources to others that have not been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. All pupils are expected to follow staff instructions including the instruction of the After School Club staff. If a pupil does not follow these, they will no longer be allowed to use the Internet.

Social sites such as Facebook only permit access to people over the age of 13yrs. These sites pose a variety of dangers to young people, therefore the school endorses the restrictions. Social sites are blocked in school; parents are asked to monitor this at home. We actively discourage children from using other social media sites and children are never allowed to access them in school as they are blocked.

Any queries relating to this policy should be addressed to Miss Atkinson, Computing Subject Leader or the Head Teacher.

Yours sincerely,

Lisa Weeks	Elizabeth Atkinson
Head Teacher	Computing and E-Safety Coordinator

Review Date: December 2018

St James’ RC Primary School
Acceptable Use Policy for Internet Access

1. School policies apply to Internet use, in particular the Safeguarding, E Safety, Computing and Equal Opportunities Policy.
2. Private use of the Internet will be agreed with the school and will be subject to the same guidelines and policies as professional use of the services being used.
3. Electronic ordering on the Internet will be in line with the financial requirements and procedures of the schools.
4. The Internet is provided for the purpose of research and communication and its use will be limited to this purpose.
5. All children in all year groups will be taught in an age appropriate way how to access the internet safely.
6. Adults competent in using the Internet will supervise **all** pupil Internet sessions.
7. Access will always be in 'public' areas where screens are visible. Internet use will be driven by clear learning intentions, which are set in the context of well framed tasks.
8. Pupils will not be given access to Newsgroups or 'chat areas.’
9. No personal details will be given out over the Internet except in carefully approved circumstances (e.g. joint projects). This will always be administrated and organised by a class teacher.
10. The school will keep its anti-virus software up to date to ensure that school activities are not disrupted by the malevolent actions of others. The implementation of this policy will be formally monitored by the school with details of upgrades being logged by the school and implemented by our ICT support provider.
11. Pupils receiving questionable materials will report these immediately to the supervising adult. All children will be taught what to do if they see something inappropriate on the internet.
12. Particular care will be taken when performing Internet searches as the search engine may accidentally return undesirable links. Teachers will always search using the same vocabulary as the children before the session to ensure that the results are appropriate.
13. All Internet users will be aware that all access is logged, and that any material accessed may subsequently be viewed by other users as well as the system administrator.
14. The school will enter into a "contract" with pupils and parents to regulate Internet use.
15. School will enter into a contract with staff to regulate the use of the Internet.
16. The school's personal computers (including portables) will only be used to access the Internet through an officially authorised route.
17. Any software downloaded from the Internet on to computers or tablets will be appropriately virus checked, licensed and registered. (Authority for this is only given to I.C.T. Subject Leader).
18. School staff will not accept pupils or past pupils of school age onto their social sites.
19. Portable devices including those that are hand held must be handed in to the school office first thing in the morning and collected at the end of the day. Mobile phones are kept under lock and key for those pupils in Year 6 who walk to school. Mobile phones that have any kind of internet capability will not be allowed on the school premises.
20. The school will manage the website with due care and attention.

Review Date: December 2018

St James' RC Primary School

Acceptable Use Policy for Internet Access

Pupil and Parental Permission Form

Please read through these guidelines with the children, explaining and answering any questions they may have.

1. I will not log on to the Internet without the direct permission of a member of staff.

2. I will follow the instructions of the teacher at all times.

3. I will not send or display inappropriate messages or pictures.

4. I will not knowingly search for inappropriate material on the Internet.

5. I will not copy or down load anybody else's work from the Internet.

6. I will not use another person's password.

7. I will not open up another person's file or folder without permission from the teacher.

8. I will not print unnecessary files or pictures.

9. I will not knowingly introduce a virus onto the school system.

10. I will not contact any member of staff via any social media site.

Declaration

I have seen the rules, which apply to using the Internet and I understand that if I break any of these rules I will lose my access to the use of the Internet and further action may need to be taken.

The teaching staff check the use of the Internet and a record is kept on the school system.

Pupil's Signature and Date: ____

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to access networked computer services such as electronic mail and the Internet.

I understand that some materials on the Internet may be objectionable, but I accept responsibility for my daughter or son to follow the above stated rules when selecting, sharing and exploring information and media.

Parent's Signature and Date: ___________________________________

Review Date: December 2018

APPENDIX 2 ACCEPTABLE USE POLICY FOR STAFF

St James' RC Primary School

Acceptable Use Contract for Staff

As a member of staff at St. James' RC Primary School I agree to adhere to the Christian ethos of the school and to the high professional standards that are expected.

In respect of internet use I agree that I will act responsibly in my dealings with young people at all times. This means that:-

- I will not allow current pupils or past pupils still of school age permission to access my social sites
- I will not post pictures of pupils or of any school activity on my social site
- I will not discuss or refer to my work in school on my social site
- I will not discuss a pupil with a parent on my social site
- I will not contact pupils or past pupils of school age via any social network
- I will not post pictures of myself or colleagues in an undignified situation
- I will not use unsuitable language or make distasteful comments on my social site
- I will not photograph children in school without the permission of the Head Teacher
- I will not download pictures of pupils onto my home computer

Declaration

I have seen the rules, which apply to the private and professional use of the internet and agree to abide by them. I understand that my actions affect the safety of the pupils as well as the ethos and reputation of the school. A breach of the above rules could lead to dismissal

Staff Signatureand Date:

____