****

**E-Safety Policy 2018 – 2019**

**1. Introduction and Overview**

**Rationale**

**The purpose of this policy is to:**

1. Set out the key principles expected of all members of the school community at St John of Jerusalem COE Primary School with respect to the use of ICT-based technologies.
2. Safeguard and protect the children and staff of St John of Jerusalem COE Primary School
3. Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
4. Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
5. Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
6. Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
7. Minimise the risk of misplaced or malicious allegations made against adults who work with students.

**Scope** (from SWGfL)

This policy applies to all members of St John of Jerusalem COE Primary School community (including staff, students / pupils, Governors, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy ICT systems, both in and out of St John of Jerusalem COE Primary School.

**The Education and Inspections Act 2006** empowers Head teachers / Principals to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the schoolsite and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school / academy, 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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

**Our vision**

At St John of Jerusalem COE Primary School all our pupils are our paramount concern. Our aim is that all pupils learn to their full potential, in a safe and enjoyable environment. As such, we take the safeguarding of our children very seriously. This E-Safety Policy must be read in conjunction with our Safeguarding and Behaviour Policy.

**Risks associated with use of ICT based technologies;**

In a world that uses ICT based technologies in most aspects of life, it is important that staff and pupils use them safely and responsibly. This is due to the potential risk associated with its use. The main areas of risk to the school and wider school community are:

1. Cyberbullying – which covers use of mobile phones;
2. Exposure to inappropriate content, including age related games;
3. Use of digital pictures in terms of copyright;

**School Approach**

With this in mind and to ensure that all our pupils and staff understand and know how to use the internet and technological devices safely and responsibly, we hold annual training workshops on E-Safety. As well as this, we termly have updates in our Newsletters, giving staff, pupils and parents’ useful information and tips. We also participate in the **Safer Internet Day** programme of learning once a year. This involves each class completing several sessions of drama, discussions and writing linked to E-Safety.

**Class Approach**

During all subjects where ICT technology is used teachers regularly remind pupils of the E-Safety rules. Pupils are also reminded when sharing these devices to always report any inappropriate content to their teacher. If this is the case, then the teacher will then follow the procedure for reporting such content. All classes have displays about E-Safety again to reinforce this important topic.

Teachers must ensure that any website used for learning by either themselves or the pupils is appropriate and enhances the learning of the children. Extra- curricular activities like homework, teachers must ensure that they give pupils appropriate websites to carry out research.

Pupils in Key Stage 2 use The ‘London Grid For Learning’ secure page to access class blogs. To ensure that only appropriate material is published, the teacher must read all posts before agreeing to publish a pupil’s work.

Ultimately, the aim in class is that the use of IT enhances and supports the children’s learning. By following the above, pupils learning will be enriched.

**Staff/Volunteer training**

All teachers and other support staff receive E-Safety training by either external experts and or designated staff members. All staff, including volunteers read and sign **An Acceptable Use Policy** annually, which ensures that our data and staff knowledge and understanding on this important area is kept up to date.

**Pupil training**

All pupils, from Nursery to Year 6 receive annual training on E-Safety according which is appropriate to their specific age and usage of the internet and other technological devices. Pupils are taught a range of skills to support them in using a device responsibly. Throughout all years, the pupils Acceptable User Policy focus is on: **Think before You Click.** All children from reception to year 6 have signed to state that they will use ICT technologies safely and responsibly.

**Roles and Responsibilities**

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school Governors / Board of Directors:

*Governors / Directors* are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors / Directors / Sub Committee* receiving regular information about e-safety incidents and monitoring reports. A member of the *Governing Body / Board* has taken on the role of *E-Safety Governor* / *Director The role of the E-Safety Governor / Director will include:*

*• regular meetings with the E-Safety Co-ordinator / Officer*

*• regular monitoring of e-safety incident logs*

*• regular monitoring of filtering / change control logs*

*• reporting to relevant Governors / Board / committee / meeting*

***Headteacher / Principal and Senior Leaders:***

*•* ***The Headteacher / Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community****, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator / Officer.*

*•* ***The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.*** *(see flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / other relevant body disciplinary procedures).*

*The Headteacher / Principal / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry*

their e-safety roles and to train other colleagues, as relevant.

***Child Protection / Safeguarding Designated Person / Officer***

*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 Support Staff***

*are responsible for ensuring that:*

***• they have an up to date awareness of e-safety matters and of the current school / academy e-safety policy and practices***

***• they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)***

***• they report any suspected misuse or problem to the Headteacher / Principal / Senior Leader ; E-Safety Coordinator / Officer*** *(insert others as relevant)* ***for investigation / action / sanction***

***• all digital communications with students / pupils / parents / carers should be on a professional level*** *and only carried out using official school systems*

*• e-safety issues are embedded in all aspects of the curriculum and other activities*

*• students / pupils understand and follow the e-safety and acceptable use policies*

*• students / pupils 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 students / pupils 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*

***Students / pupils:***

***• are responsible for using the school / academy digital technology systems in accordance with the Student / Pupil Acceptable Use Policy***

*• 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 taking / use of images and on cyber-bullying.*

*• should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s / academy’s E-Safety Policy covers their actions out of school, if related to their membership of the school*

**Handling complaints:**

* The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
* Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  + interview/counselling by tutor / Head of Year / E-Safety Coordinator / Headteacher;
  + informing parents or carers;
  + removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
  + referral to LA / Police.
* Our Safe guarding Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
* Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

**Review and Monitoring**

The e-safety policy is referenced from within other school policies: ICT and Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

* The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
* The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
* The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
* There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

**Parents / Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school / academy* will take every opportunity to help parents understand these issues through *parents’ evenings, newsletters, letters, website / and information about national / local e-safety campaigns / literature.* Parents and carers will be encouraged to 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 / VLE and on-line student / pupil records

• their children’s personal devices in the school / academy (where this is allowed).