St Alban's Catholic Primary School

E-SAFETY POLICY

Title:	**E-Safety Policy**
Policy Agreed:	**January 2017**
Next Review:	**January 2018**

Table of Contents

1. MISSION STATEMENT 3
2. Introduction 3
3. Purpose 4
4. Ofsted Report 4
5. Teaching and Learning 4
   5.1 Pupils will be taught how to evaluate Internet content 5
6. Managing Internet Access 5
   6.1 Information system security 5
   6.2 E-mail 5
   6.3 Published content and the school website 5
   6.4 Publishing Pupils' images and work 6
   6.5 Social networking and personal publishing on the school learning platform 6
   6.6 Managing filtering 6
   6.7 Managing emerging technologies 7
7. Policy Decisions 7
   7.1 Authorising Internet access 7
   7.2 Assessing risks 7
   7.3 Handling E-safety complaints 8
   7.4 Community use of the Internet 8
8. Communications Policy 8
   8.1 Introducing the E-safety policy to pupils 8
   8.2 Staff and the E-safety policy 8
   8.3 Enlisting parents' support, implementation and compliance 9

APPENDIX 1 – What to do if you have an E-Safety concern? 10

APPENDIX 2 – List of Staff 11

1. MISSION STATEMENT

The new mission statement for St. Alban's was created by the children, staff, parents and governors of the school.

We in St. Alban's Catholic Primary have a primary responsibility for the care, welfare and safety of the pupils in our charge. We aim to provide a caring, supportive and safe environment, valuing individuals for their unique talents and abilities, with the aim that all young people can learn and develop to their full potential.

2. Introduction

The E-safety Policy is part of the School Development Plan and relates to other policies including those for computing, bullying and for child protection. This policy is not about policing children but rather protecting them from abusive and criminal activity on the Internet.

- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The E-safety Policy and its implementation will be reviewed annually.
- The E-safety Policy was revised by the Computing Lead.

3. Purpose

The Internet is a fantastic resource that enables learning in a huge range of ways. It is an integral part of modern, western society and impacts on most areas of life. To this end it is important that all young people are confident in using this resource but have the appropriate tools to stay safe and protected whilst doing so. The purpose of this policy is to ensure that the content that pupils are exposed to on the internet, the contact pupils have with others via ICT systems and pupils' conduct whilst online are all suitable and afford them the opportunity to explore ICT and the internet in a confident, safe and secure manner that aids their learning and development.

If you have an E-safety concern, please refer to Appendix 1 for the procedure to follow.

4. Ofsted Report

In the most recent Ofsted report dated December 2012, it was stated that the safety of our pupils is good and 'the older pupils are aware of Internet dangers'.

5. Teaching and Learning

- The Internet is an unmanaged essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils (e.g. for research and resources to enhance learning). Each class will have an allotted slot in the Computer suite; they will also be able to use laptops and tablets within the classroom for Computing lessons and for other curriculum areas.

- The school Internet access is provided by RM Education through RM SafetyNet Plus filtering by SEGFL and includes user based filtering, appropriate to the age of our pupils.

- The school employs a robust user monitoring system through Securus software that automatically monitors all electronic activity (internet and application based) both within and outside places of learning, ensuring that our pupils are safeguarded against the wide range of threats they face in the digital age. Securus flags and records any internet/application violation to the ICT support staff and safeguarding team, taking a screen capture and recording the user name and date/time of any viewing/access of inappropriate material. Securus captures are monitored on a daily basis by the child protection and safeguarding team.

- Using both RMSafetyNet Plus and Securus the school aims to make lasting improvements in pupil behaviour and safety by helping pupils to recognise unsafe situations through making mistakes in a safe environment.

- Pupils will be taught what Internet use is acceptable and what is not; they will be given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

5.1 Pupils will be taught how to evaluate Internet content

- Pupils will be taught to be critically aware of the materials they read; they will be shown how to validate information before accepting its accuracy.
- Pupils will be taught, through E-Safety lessons, what to do if they come across material that they feel is unacceptable or inappropriate.

6. Managing Internet Access

6.1 Information system security

- School ICT systems will be reviewed annually. The Internet/broadband is from RM Education.
- Anti-virus software is updated regularly by Sophos End Point Security and Control Software.
- Security strategies (E- Safety, Staff Acceptable Use Policy and Parent/Pupil Acceptable Use Policy) will be compliant with the Local Authority e-safety standards.

6.2 E-mail

Pupils and staff may only use approved e-mail accounts on the school system.

- Pupils must immediately tell a teacher if they receive any offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Any e-mails from pupils to external bodies will be sent from a teacher's account and the email monitored and sent by the teacher.
- The forwarding of chain letters is NOT permitted.

6.3 Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher, Computing Lead and IT technician will take overall editorial responsibility and ensure that all content on the website is accurate and appropriate.

6.4 Publishing Pupils' images and work

- Photographs that include pupils will be selected carefully for display on the website.
- Pupils' full names will not displayed be on the school website.
- Written permission from parents or carers will be obtained before photographs are published on the school website; each register contains a list for the appropriate class.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories, refer to the 'Acceptable Use Policy (Parent/Pupil)' and 'Using Photographic Images of Children' Policies.

6.5 Social networking and personal publishing on the school learning platform

- The school will not allow access to social networking sites (for example 'Facebook' or 'MySpace').
- When newsrooms are needed they will be assessed prior to a lesson to make sure that the content is age appropriate and does not contain any visually upsetting images.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location including the use of passwords.
- Pupils must only publish approved personal photos on any social network space provided in the school learning platform, for example photos of trips.
- Pupils and parents will be advised that the use of social network sites outside school brings a range of dangers for all pupils, particularly those of primary age. However, the school can only recommend and not enforce that pupils do not use outside social networking sites.
- Pupils will be advised to use nicknames and avatars (a graphical representation of the user) when using school approved educational social networking sites e.g. Mathletics uses avatars which the children can create and dress up.

6.6 Managing filtering

- The school will work in partnership with RM Education, Securus and Surrey County Council to ensure systems in place to protect pupils are regularly reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the IT Technician. In the first instance, the report-abuse form (kept within the ICT suite folder) must be filled in documenting the date, child, year group, offending website and the action taken by the teacher. The form must then be passed to the Designated Safeguarding Lead (DSL) and IT Technician (see Appendix 2).
- Senior staff, along with the IT technician, will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The ICT technician is able to allow access to blocked Internet sites at the request of a teacher for a certain lesson.

6.7 Managing emerging technologies

- Emerging technologies will be examined for educational benefit; a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons or formal school time, except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden and if sent the relevant agencies may be informed.
- Staff will use a school phone where contact with parents is required (except school trips where a mobile may be used, 141 is advised).

7. Policy Decisions

7.1 Authorising Internet access

- All staff must read and sign the 'Staff Acceptable Use Agreement" before using any school ICT resource. The Staff Acceptable Use Agreement will include staff's own social media responsibilities.
- The school will maintain an up to-date record of all staff and pupils who are granted access to school ICT systems. Any new child who needs to be included will be added by the IT technician and assigned the appropriate access and usage permissions.
- At Key Stage 1, access to the Internet will be by adult demonstration, with directly supervised access to specific, approved on-line materials.
- From September 2013 all new parents and pupils will be asked to sign the 'Parent/Pupil Acceptable Use Policy'.
- Any person not directly employed by the school will be asked to sign a 'visitor acceptable-use agreement/code of conduct' before being allowed to access the Internet from the school site.

7.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material from within the school premise and internet access. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will continually evaluate computing use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

7.3 Handling E-safety complaints

- Complaints of Internet misuse by a pupil will be dealt with in the first instance by the IT Technician and then passed on to the Headteacher.
- Any complaint about staff misuse must be referred directly to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures.
- Pupils and parents will be informed of consequences for pupils misusing the Internet, through the use of curriculum evenings and newsletters where appropriate.

7.4 Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

8. Communications Policy

8.1 Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety policy will be shared with pupils.
- The E-safety SMART rules, which have been written by the pupils following their E-Safety unit of work, will be displayed in the ICT suite.
- Pupils will be informed that network and Internet use will be monitored.
- All children in KS1 and KS2 will cover an E-Safety unit in the Autumn term, providing opportunities for them to gain age-related awareness of E-safety issues and how best to deal with them.

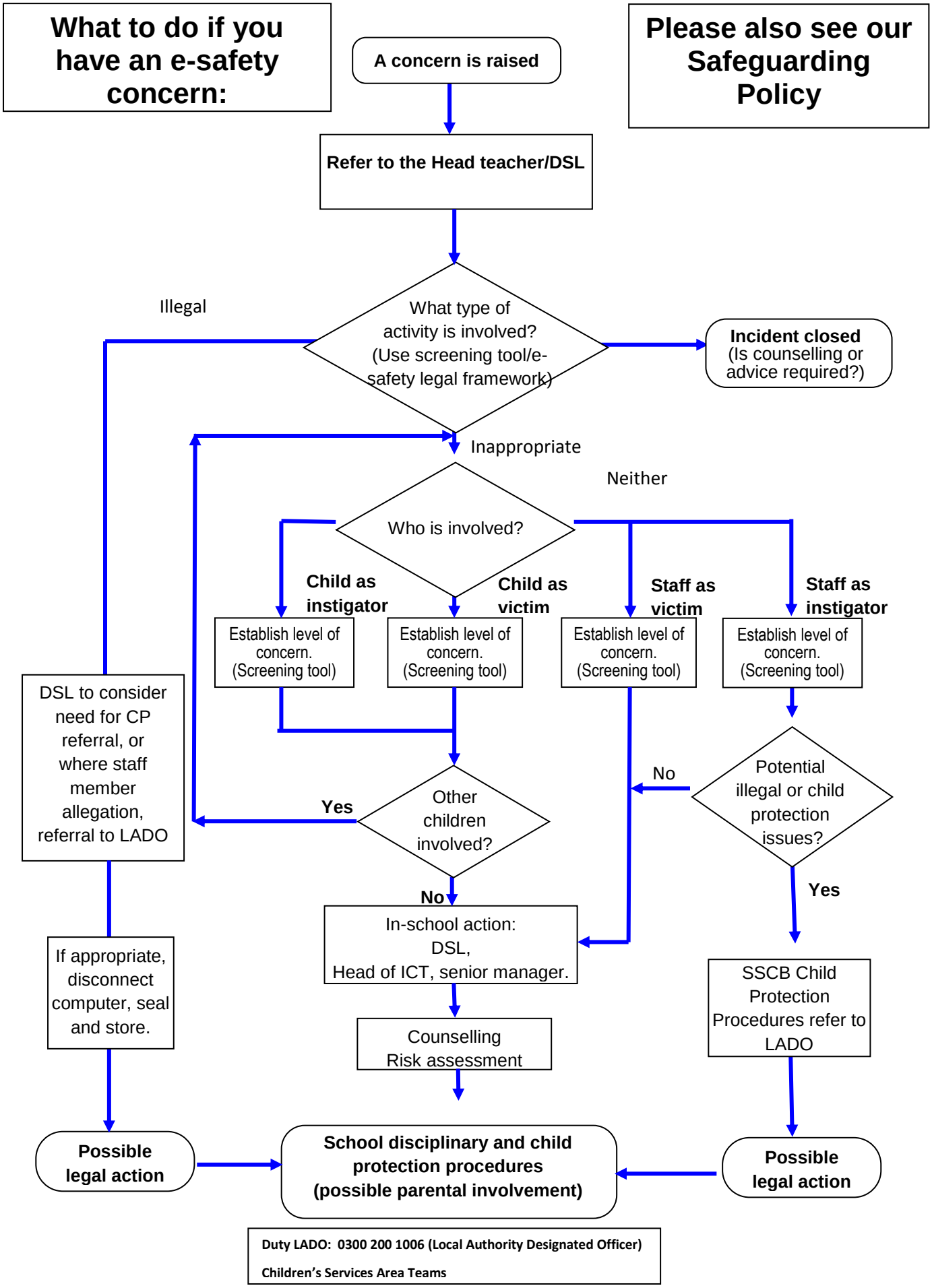
8.2 Staff and the E-safety policy

- All staff will be given sufficient and regular training to an appropriate level to allow them to identify e-safety issues.
- All staff will be given the E-safety policy and its importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and will have clear procedures for reporting issues.
- Staff mobile devices, if used on the premises, will not be allowed to use the school wireless network.

8.3 Enlisting parents' support, implementation and compliance.

- Parents and carers attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school website.
- Parents and carers will from time to time be provided with additional information on E-safety e.g. Internet Safety Week, E-Safety parent workshops and E-Safety leaflets.
- From September 2013 the school will ask all new parents to sign the Parent/Pupil Acceptable-Use Policy agreement when they register their child with the school.

APPENDIX 1 – What to do if you have an E-Safety concern?



APPENDIX 2 – List of Staff

Role	Staff Name
Designated Safeguarding Leads (DSL) & Prevent Officers	Mrs Jane Bishop (Deputy Head) Mr Martin Brannigan (Headteacher) Mrs Elaine Holliday (SEN Manager)
IT Technician	Mrs Fiza Rasool
Computing Lead	Mrs C Martin