St Margaret's Lee Church of England Primary School

E-Safety Policy

Date:	May 2017	Review Date:	May 2018

Our Mission Statement:

- We have high expectations of everyone.
- We believe every child can and should achieve.
- We want children to be happy and safe in our caring, Christian community.
- We go the extra mile.

Contents:

Our e-Safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It will be reviewed annually.

Whole school approach to the safe use of technology

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.

Reference: Becta - E-safety Developing whole-school policies to support effective practice [1]

Roles and Responsibilities

e-Safety is recognised as an essential aspect of strategic leadership in this school and the headteacher, with the support of governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the policy is implemented and in compliance with the policy monitored.

Our school **e-Safety Co-ordinator** is Ian Wilson

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP)[2]. The school's e-Safety coordinator ensures the headteacher, senior leadership and governors are updated as necessary.

[1] http://schools.becta.org.uk/index.php?section=is
[2] http://www.ceop.gov.uk/

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance [3] on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs and use of website;
- Cyberbullying procedures;
- Their role in providing e-Safety education for pupils;

How will complaints regarding e-Safety be handled?

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:

- Discussion with 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]
- Referral to LA / Police.

Using the internet

Why Internet use is important

- The Internet is an 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.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and 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
- When appropriate the school will use 'safer' search engines with pupils such as http://yahooligans.yahoo.com/ | http://www.askforkids.com/ and activates 'safe' search where appropriate;
- The school Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;

[3] Safety and ICT - available from Becta, the Government agency at:
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=10247

Education programme:

At St Margaret's:

- children are encouraged to tell a teacher or responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- we ensure pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or e-safety co-ordinator
- children are taught how to evaluate internet content and to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- **e-safety** is taught using the CEOP www.thinkuknow.co.uk/ at Key Stage 1 and 2
- we deliver support to parents who have an important role in supporting safe and effective use of the internet by pupils (This is done by 'drip-feeding' information via the newsletter and school website)
- staff are trained annually on the e-safety education program;
- pupils and staff know what to do if a cyber-bullying or other e-safety incident occurs;

Managing Internet Access

Information system security

This school:

- Maintains broadband connectivity through the LGfL and so connects to the National Education Network;
- Ensures virus protection will be updated regularly.
- Uses class log-ins for pupils

We use the pan-London LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature; Informs staff and students that that they must report any failure of the filtering systems directly to the [*system administrator / teacher / person responsible for URL filtering]*. Our systems administrators report to LA / LGfL where necessary.

This school:

- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only uses approved blogging or discussion sites, such as on the LGfL / approved Learning Platform and blocks others.
- Only uses approved or checked webcam sites;

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Parents will be asked to sign and return a consent form.

Email

Pupils:

- Pupils do not currently have access to a school email account

Staff

- Staff use the LGfL / school domain e-mail accounts or web-based email for professional purposes
- use of personal email accounts is not permitted

Images

- Digital images /video of pupils are stored in the media drive on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication.
- We do not use pupils' names when saving images in the file names
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs.
- All staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school;

Using the school network

This school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Provides pupils with a class network log-in username;
- Makes it clear that staff must keep their log-in username and password private and must not leave them where others can find;
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used to support their professional responsibilities

How will infringements be handled?

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school leadership.

The following are provided as exemplification only:

Children

Category A infringements:

- Use of internet for non-teacher directed activities (except for agreed websites – cbeebies/cbbc, mathletics)
- Mobile phones (or other new technologies) left on in bags
- Use of mobile phones on school grounds

[Sanctions: referred to class teacher, if repeated referred to Senior Leadership resulting in parents being informed and an agreed sanction put in place]

Category B infringements:

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet

[Sanctions: referred to Senior Leadership/parents informed]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform LA / LGfL as appropriate

Category C infringements:

- Sending of emails or MSN messages regarded as harassment or of a bullying nature
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988

[Possible Sanctions* – Referred to Headteacher / parents informed/victim's parents informed/ *possible exclusion / removal of equipment / refer to Community Police Officer / LA e-safety officer]

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

<u>Staff</u>

- Serious misuse of, or deliberate damage to, any school computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

[Sanction – Referred to Headteacher / Governors and follow school disciplinary procedures; report to LA Personnel/ Human resources, report to Police]

Other safeguarding actions:

1. Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.

2. Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
3. Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child Pornography found?

In the case of Child Pornography being found, the member of staff should be **immediately suspended** and the Police should be called: **0808 100 00 40** at: http://www.met.police.uk/childpornography/index.htm

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's e-safety / Acceptable Use Policy.;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate acceptable use form;
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on e-safety issues, (see LGfL safety site).