*St Gabriel's E-SAFETY Policy*

**Date:** Spring 2017
**Lead Person:** H.Gilbert
**Committee:** Policy
**Date of next review:** Spring 2018

## *1.* Development of this Policy

The e–Safety Policy and its implementation will be reviewed annually.
• Our e–Safety Policy has been written by the ICT co-ordinator, building on the Kent County Council e–Safety Policy and government guidance.
• Our School Policy has been agreed by the Senior Leadership Team and approved by governors and other stakeholders

## 1.1 Schedules for Development and Review

| | |
|---|---|
| This e-safety policy was approved by the Governing Body | |
| The implementation of this e-safety policy will be monitored by the: | *E-Safety Coordinator and Senior Leadership Team* |
| Monitoring will take place at regular intervals: | Termly by ICT co-ordinator |
| The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group which included the e-safety co-ordinator, the Head teacher and the safe guarding governor (which will include anonymous details of e-safety incidents) at regular intervals: | ICT co-ordinator reporting back to safe guarding governor and the Head teacher termly. |
| The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | *Autumn 2017* |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | *Police , CEOP-* 0870 000 3344 |

# 2. Teaching and learning

**Why is Internet use important?**

•Internet use is part of the statutory curriculum and is a necessary tool for learning. The school has a duty to provide students with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

• The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

• Internet access is an entitlement for students who show a responsible and mature approach to its use.

**How does Internet use benefit education?**

Benefits of using the Internet in education include:
• access to worldwide educational resources including museums and art galleries;
• inclusion in the National Education Network which connects all UK schools;
• educational and cultural exchanges between pupils worldwide;
• vocational, social and leisure use in libraries, clubs and at home;
• 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 networks of schools, support services and professional associations;
• improved access to technical support including remote management of networks and automatic system updates;
• exchange of curriculum and administration data with *Westminster and Tri-borough*

**How can Internet use enhance learning?**

• The school's Internet access will be designed to enhance and extend education. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

• Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.

• 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 taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

•A planned e-safety curriculum should be provided as part of Computing / PSHE / other lessons and should be regularly revisited

•Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities

**How will pupils learn how to evaluate Internet content?**

-Pupils will use age-appropriate tools to research Internet content.

-Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

-Students / pupils should be helped to understand the need for the student /pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

•Staff should act as good role models in their use of digital technologies the internet and mobile devices

## Managing Information Systems

**How will email be managed?**

•Our e-mail is provided by lgfl found at https://mail.lgflmail.org
Each member of staff has their own e-mail address, which is adequate to meet the requirements of the National Curriculum. Our e-mail addresses are composed of the initial letter of the first name followed by surname (all in lower case letters), for example Joe Blogs becomes:**jblogs@stgabrielsprimary.co.uk**
There is an administrator account through which the technician can add users from the address. The administrator has a password for this account.
Messages sent using the school domain name should be regarded in the same way as messages written on school headed paper.  Pupils will be made aware that emails are subject to the same standards of etiquette as any other form of communication and should be polite and use appropriate language.  Anonymous emails will be deleted.  The forwarding of chain letters will be banned, as will the use of chat-rooms.

• Unapproved software will not be allowed in work areas or attached to email.
 Files held on the school's network will be regularly checked.

•The ICT coordinator/network manager will review system capacity regularly.

• The use of user logins and passwords to access the school network will be enforced.

• Personal data sent over the Internet or taken off site will be encrypted.

•The security of the school information systems and users will be reviewed regularly.

•Pupils may only use approved email accounts for school purposes.

•Pupils must immediately tell a designated member of staff if they receive offensive email.

•Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

•Whole -class or group email addresses will be used in primary schools for communication outside of the school.

•Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team

•Access in school to external personal email accounts may be blocked.

•Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.

• The forwarding of chain messages is not permitted.

**How will published content be managed?**

•Our school has its own website, to be found at http://www.stgabrielsprimary.co.uk
The point of contact on the web-site is the school address and the telephone number. Home information or individual email identities are not published. It will be the responsibility of the senior school administrator to ensure that the web-site is kept up-to-date and that all out-of-date material is removed promptly.

**Can pupils' images or work be published?**

•Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

•The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright

•Group shots or pictures taken over the shoulder should be used in preference to 'portrait' style photographs

•Written permission from parents must be obtained before any photographs of pupils are published on the school web-site.

•Pupils work can only be published with their permission and the parents.

•The School has a policy regarding the use of photographic images of children which outlines policies and procedures.

**How will social networking, social media and personal publishing be managed?**

•Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests and clubs etc

•Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.

•Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

•Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

•Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

- Annual audit of safety and security of school systems takes place with the Head Teacher and architect.

- ACTSOLUTIONS currently provide the school with technical support. A member of technical staff monitors and oversees infrastructure, equipment, filtering and monitoring of ICT devices.

- A secured Wi-Fi has been implemented throughout school and is filtered through LGFL

## Protection for Users of the Internet at St. Gabriel's School

**How will protection for users of the internet be managed?**

All users of the Internet at St. Gabriel's School will be protected from the risks in the following ways:

1. Internet access is provided by LGfL who operate a filtering service appropriate to primary schools.
2. All school use of the Internet, including that by pupils, teachers, other members of staff, Governors and parents will be monitored.
3. The co-coordinator will immediately report any unsuitable material found on the Internet to the service provider who will then block access to the address as reported.
4. Full names, home addresses and telephone numbers of pupils or members of staff, personal information or photographs identifying individuals will <u>never</u> be made available over the Internet.
5. Use of public chat-rooms will not be permitted.
6. New facilities will be thoroughly tested before pupils are given access to them.
7. Rules for the responsible use of the Internet will be displayed near all computers with Internet access.
8. All members of staff including teachers, supply teachers, support staff and classroom assistants will be made aware of the issues surrounding Internet access. Staff sign an acceptable use policy document.
9. The school will offer sessions for parents on the responsible use of the Internet at home.
10. All children will be taught on e-safety. Staff have had training in e-safety and ideas for planning an e-safety lesson is in the shared area. All children and staff sign an acceptable use agreement at the beginning of the year.

**What sanctions following the misuse of the internet will occur?**

Any user of the Internet who violates the school rules on responsible use will be dealt with very seriously. Sanctions could include:

1. Temporary or permanent removal of entitlement to use email, access to the Internet or use of computers and other I.C.T. equipment at school.
2. A letter to parents, Governors and or the Local Authority informing them of the nature of the violation.
3. In the case of violation by any member of staff disciplinary action may be considered.
4. In extreme cases the use of computer systems without permission of for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990 and may be reported to the police.

**How are emerging technologies managed?**

•Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

• Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.

**How should personal data be protected**?

•Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

**How will the school respond to any incidents of concern?**

•The Designated Safeguarding officer will collect and record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.

•The Designated Safeguarding officer will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

•The school will manage e-Safety incidents in accordance with the school behaviour policy where appropriate.

•The school will inform parents/carers of any incidents of concerns as and when required.

•After any investigations are completed, the school will debrief, indentify lessons learnt and implement any changes required.

•Staff training will be provided to ensure that staff are aware of reporting abuse protocol and using CEOP.

•Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact CEOP and escalate concerns to the police.

**How will Cyberbullying be managed?**

•Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

•The Police will be contacted if a criminal offence is suspected.

•Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.

•Parent/carers of pupils will be informed.

**How will Learning Platforms be managed?**

•SLT and staff will regularly monitor the usage of any Learning platforms or Class blogs by pupils and staff in all areas, in particular message and communication tools and publishing facilities.

•Pupils/staff will be advised about acceptable conduct and use when using the LP/blog.

•Only members of the current pupil, parent/carers and staff community will have access to the LP/Blog which is ultimately controlled by the class teacher who has administration rights. Blogs may be viewed outside of this community but will be strictly monitored by the Class teacher who will monitor any comments before they are able to be posted.

•Any concerns about content on the LP/Blog may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the LP for the user may be suspended.
d) The user will need to discuss the issues with a member of SLT before reinstatement.
e) A pupil's parent/carer may be informed.

•Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame

**How will mobile phones and personal devices be managed?**

The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in AUP.

**Pupils Use of Personal Devices**

Any personal devices brought in my students are brought into the office for safe keeping and picked up at the end of the school day.

**Staff Use of Personal Devices**

•Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

• Staff will be issued with a school phone where contact with pupils or parents/carers is required.

• Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.

• If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team

• Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

• Educational software via devices such as IPADS and smart phones may be used in classrooms

after being approved by senior leadership team.

• If a member of staff breaches the school policy then disciplinary action may be taken.

# Communication Policy

**How will the policy be introduced to pupils?**

• Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

• Particular attention to e-Safety education will be given where pupils are considered to be vulnerable. For example looked after children and children with SEND needs such as ASD.

**How will the policy be discussed with staff?**

•The e–Safety Policy will be formally provided to and discussed with all members of staff

**How will parents' support be enlisted?**

• Parents' attention will be drawn to the school e–Safety policies in the following ways throughout the year:

- Curriculum activities
- Letters, newsletters, web site, Class blogs
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g Safer Internet Day
- Reference to the relevant web sites / publications e.g
*www.saferinternet.org.uk/*   *http://www.childnet.com/parents-and-carers*

## Schools e-Safety survey

• A survey for children to gather information about e-safety knowledge and usage of technology at home and school will be carried out using guidelines as featured in LGFL e-safety survey.

## Complaints

Any complaints regarding use of the Internet in St. Gabriel's School should be made promptly to the Head Teacher or ICT co-ordinator. All complaints will be treated seriously and will be dealt with immediately.

## Disclaimer

St. Gabriel's School has taken all reasonable precautions to ensure that users of the Internet have access to appropriate material only.  All staff, Governors, parents and pupils will work together to ensure that every reasonable measure is implemented on a day-to-day basis to promote responsible use of the Internet.  However, due to the nature of the Internet it is not possible to guarantee that unsuitable material will never appear on a computer screen in the school.  St. Gabriel's School, Westminster L.A. and LGfL cannot accept liability for the materials accessed or the consequences there of.  Nor can parents hold us responsible for unacceptable use of the Internet by pupils when using the Internet in any context outside the school.

## Contacts and references
CEOP (Child Exploitation and Online Protection Centre)**: www.ceop.police.uk**

**Childline**: www.childline.org.uk

Childnet**: www.childnet.com**

Kidsmart**: www.kidsmart.org.uk**

Think U Know website**: www.thinkuknow.co.uk**

Schools e–Safety Blog**: www.kenttrustweb.org.uk?esafetyblog**


**Technical glossary:**
VLE- virtual learning environment


## Appendices


**Appendix 1:  'Rules for the Responsible Use of the Internet' Poster.**

**Appendix 2:' Responsible use of the internet rules for children.**

**Appendix 3:  Request letter to parents asking for permission to use a photograph of their child on the school web site.**

**Appendix 4: Acceptable Use Policy for Staff.**

**Appendix 5: Request letter for parents asking permission to use photographs or work of their children on class blog.**

# St Gabriel's C.E Primary School
## Rules for Responsible Internet Use

- *Always ask permission to use the Internet.*
- *Only use the Internet when there is an adult in the room.*
- *Never use the Internet alone.*
- *Never pretend to be someone else, use another person's name or read other people's files when using the Internet or sending e-mail.*
- *Never use the Internet or e-mail at school in a way that could cause upset to others.*
- *Only use the Internet for educational purposes.*
- *Do not use USB's/CD'sfrom home unless a teacher has given you permission.*
- *Never download programs from the Internet or load your own software unless permission has been granted by your teacher.*
- *Never use a chat-room on the Internet in school.*
- *Only e-mail people your teacher has approved.*
- *Never give out your full name, home address or telephone number of any children or staff without your teacher's permission.*
- *Never put a photograph of yourself or another child or member of staff onto the Internet or e-mail without permission.*
- *Only write sensible and polite messages and report any unpleasant messages to your teacher immediately.*
- *Tell a teacher if your see anything on a computer screen that you do not feel comfortable with or anything that you know you should not be allowed to see.*
- *Never arrange to meet someone in person that you have communicated with on the Internet without talking to your teacher about it first.*

*( display in classroom )*

# St Gabriel's C.E Primary School
# Rules for Responsible Internet Use

- *Always ask permission to use the Internet.*
- *Only use the Internet when there is an adult in the room.*
- *Never use the Internet alone.*
- *Never pretend to be someone else, use another person's name or read other people's files when using the Internet or sending e-mail.*
- *Never use the Internet or e-mail at school in a way that could cause upset to others.*
- *Only use the Internet for educational purposes.*
- *Do not use CD'S/USB's from home unless a teacher has given you permission.*
- *Never download programs from the Internet or load your own software unless permission has been granted by your teacher.*
- *Never use a chat-room on the Internet in school.*
- *Only e-mail people your teacher has approved.*
- *Never give out your full name, home address or telephone number of any children or staff without your teacher's permission.*
- *Never put a photograph of yourself or another child or member of staff onto the Internet or e-mail without permission.*
- *Only write sensible and polite messages and report any unpleasant messages to your teacher immediately.*
- *Tell a teacher if your see anything on a computer screen that you do not feel comfortable with or anything that you know you should not be allowed to see.*
- *Never arrange to meet someone in person that you have communicated with on the Internet without talking to your teacher about it first.*

Name:

Class:

Signed to agree:

Dear Parent(s),

Your child ………………………………………………………. Will be involved in projects that we would like to show on our class blog.

As part of our Internet policy we never show the full names of the children near the photograph and we need parental permission before we put photographs of children on the Internet.

Please sign and return the form below if you agree to allow your child's photograph and work to be put on our class blog.  If we do not receive the form we will not put your child's photograph or work on the class blog.

Yours sincerely,

Class teacher

| | **Name of School** | **St Gabriel's C of E Primary School** |
|---|---|---|
| | **AUP review Date** | **summer 2016** |
| | **Date of next Review** | **summer 2017** |
| | **Who reviewed this AUP?** | **Hannah Gilbert** |

## Acceptable Use Policy (AUP):  Staff agreement form

*Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.*

- *I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.*
- *I will not reveal my password(s) to anyone.*
- *I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.*
- *I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.*
- *I will not engage in any online activity that may compromise my professional responsibilities.*
- *I will only use the approved, secure email system(s) for any school business.*
  *(Which is currently: lgfl)*
- *I will only use the approved school email, school MLE or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.*
- *I will not browse, download or send material that could be considered offensive to colleagues.*
- *I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.*
- *I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.*
- *I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.*
- *I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.*

- *I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice.*

- *I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.*

- *I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.*

- *I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.*

- *I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.*

- *I will embed the school's e-safety curriculum into my teaching.*

- *I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.*

- *I understand that failure to comply with this agreement could lead to disciplinary action.*

**User Signature**

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I agree to abide by all the points above.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature ............................................................... Date......................................................

Full Name ........................................................................................................ (printed)

Job title ................................................................................................................................

School ..................................................................................................................................

**Authorised Signature (Head Teacher (primary)**

I approve this user to be set-up.

Signature ............................................................... Date......................................................

Full Name ........................................................................................................ (printed)