



## St Gabriel's online safety Policy

**Date:** Autumn 2021

**Lead Person:** S. Cooper

**Committee:** Policy

**Date of next review:** Autumn 2023


*This policy will be under a 2 yearly review.*

### 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 online safety lead, 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

St Gabriel's C of E Primary School  	Designated Safeguarding Lead (DSL) team and SLT team	Rebecca Anson Headteacher and DSL  Sonia Bell (DSL deputy)  Mark Nunn (Deputy DSL deputy)
	Online-safety lead	Suzannah Cooper
	Online-safety / safeguarding link governor	Valerie Michelet
	DPO	John Hicks
	Network manager / other technical support	Andrew Canter
	Date this policy was reviewed and by whom	Autumn 2021 S.Cooper
	Date of next review and by whom	Autumn 2023 Suzannah Cooper
	Monitoring will take place at regular intervals and reported to	

	Relevant parties	
	Should serious e-safety incidents take place, the following external persons / agencies should be informed:	<i>Police , CEOP- 0870 000 3344</i>

## 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

### **What are the main online safety risks today?**

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron’s 2008 report “Safer children in a digital world”). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three. The LGfL DigiSafe 2018 pupil survey of 40,000 pupils identified an increase in distress caused by, and risk from, content. For many years, online-safety messages have focused on ‘stranger danger’, i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced. Examples of this are the sharing of violent and sexual videos, self-harm materials, and coerced nudity via live streaming. Contact and conduct of course also remain important challenges to address.

### **Roles and responsibilities**

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

**Designated Safeguarding Lead - Rebecca Anson    Online Safety Lead – Suzannah Cooper**

**Key responsibilities** (remember the DSL can delegate certain online-safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from *Keeping Children Safe in Education 2018*):

- “The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).”
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL’s clear overarching responsibility for online safety is not compromised.

- Ensure “An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.”
- “Liaise with the local authority and work with other agencies in line with Working together to safeguard children”
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the head teacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety – the new LGfL DigiSafe [pupil survey](#) of 40,000 pupils may be useful reading (new themes include ‘self-harm bullying’ and getting undressed on camera)
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum (e.g. by use of the UKCCIS framework ‘Education for a Connected World’) and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Oversee and discuss ‘appropriate filtering and monitoring’ with governors (is it physical or technical?) and ensure staff are aware (Ofsted inspectors have asked classroom teachers about this). If you use LGfL filtering, view the appropriate filtering statement [here](#)
- Ensure the 2018 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
  - all staff must read KCSIE Part 1 and all those working with children Annex A
  - it would also be advisable for all staff to be aware of Annex C (online safety)
  - cascade knowledge of risks and opportunities throughout the organisation
  - [cpd.lgfl.net](http://cpd.lgfl.net) has helpful CPD materials including PowerPoints, videos and more

### **Governing Body, led by Online Safety / Safeguarding Link Governor – Valerie Michelet**

#### ***Key responsibilities (quotes are taken from Keeping Children Safe in Education 2018):***

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCCIS) [Online safety in schools and colleges: Questions from the Governing Board](#)
- “Ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of DSL [with] lead responsibility for safeguarding and child protection (including

online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support...”

- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL’s clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school
- “Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction [and] regularly updated [...] in line with advice from the LSCB [...] online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.” There is further support for this at [cpd.lgfl.net](http://cpd.lgfl.net)
- “Ensure appropriate filters and appropriate monitoring systems are in place [but...] be careful that ‘overblocking’ does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding”. LGfL’s appropriate filtering submission is [here](#)
- “Ensure that children are taught about safeguarding, including online safety [...] as part of providing a broad and balanced curriculum [...] Consider a whole school approach to online safety [with] a clear policy on the use of mobile technology.”

## **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 network manager will review system capacity regularly and liaise with Computing lead
- 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 online safety-lead or DSL 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 never 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.
11. Parents and carers will receive an AUP so they are informed of school policies.

## 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?

### **Data protection and data security**

**NB** This section serves to highlight general principles regarding the relationship between safeguarding and data protection / data security, and to signpost to useful information.

GDPR information on the relationship between the school and LGfL TRUSTnet can be found at [gdpr.lgfl.net](http://gdpr.lgfl.net); there are useful links and documents to support schools with data protection in the 'Resources for Schools' section of that page.

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (April 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

**“GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children’s Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, **appropriate organisational and technical safeguards should still be in place [...]** Remember, **the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding .”****

All pupils, staff, governors, volunteers, contractors and parents are bound by the school’s data protection policy and agreements, which can be found here. Further, this school makes use of the following from LGfL TRUSTnet:

### **-USO sign on for LGFT trustnet services**

Rigorous controls on the LGfL TRUSTnet network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection:

**-USO sign on for LGFT trustnet services -Sophos Anti-virus -Malware Bytes**

The headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of Microsoft office 365/ encryption to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

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

#### ***Handling online-safety concerns and incidents***

- 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, identify 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?**

*Permission for using learning platforms/class blogs that staff wish to set up for their class should be first from the DSL and clearly documented.*

- 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 and have overall administrative control.
- 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 agreed in the AUP.

### **Pupils Use of Personal Devices**

Any personal devices brought in by 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. Using memory cards organised through school in personal cameras may be permitted with prior agreement with the Headteacher/DSL.
- 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; in particular, through PSHE.
- 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.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 Online Safety Lead. 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 thereof. 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](http://www.ceop.police.uk)**

**Childline:** [www.childline.org.uk](http://www.childline.org.uk)

Childnet: [www.childnet.com](http://www.childnet.com)

Kidsmart: [www.kidsmart.org.uk](http://www.kidsmart.org.uk)

Think U Know website: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

**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. ( AUP)**

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

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

**Appendix 5: Acceptable Use Policy for parents/carers**

**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'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 you 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.*

# 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 you 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: \_\_\_\_\_

**St. Gabriel's C.E. Primary School,  
Churchill Gardens Road,  
Pimlico,  
London,  
SW1V 3AG.**

**Headteacher: Miss Anson**

**Date:**

Dear Parent(s),

Your child ..... Will be involved in projects that we would like to show on our class blog/school website/social media site.

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



**St Gabriel's CofE Primary School**  
**ICT User Agreement Policy:**  
**Staff, Volunteers, Governors & Contractors 2018**

<b>DATE APPROVED</b>	<i>April 2018</i>		
<b>REVIEW DATE Biennial</b>	<i>Spring 2019</i>  <i>This policy will normally be under a two yearly review, but with the introduction of the Data Protection Act 2019 following Brexit, the review period has been shortened in the first instance.</i>		
<b>SIGNED HEAD TEACHER</b>		<b>DATE</b>	
<b>SIGNED CHAIR OF GOVERNING BODY</b>		<b>DATE</b>	

**Contents**

1. Aims & Background .....	17
2. User Requirements .....	17
3. Links with Other Policies .....	20
4. Agreement Form .....	21

## **1. Aims & Background**

*This ICT user agreement covers the use of all digital technologies while in school: i.e. email, internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, apps and other relevant digital systems provided by the school or Local Authority, or other information or systems processors.*

*This ICT user agreement also covers school issued equipment (as logged on the asset register) when used outside of school, use of online systems provided by the school such as VPN or webmail, or other systems providers when accessed from outside school.*

*This ICT user agreement also covers posts made on any non-school official social media platform or app, made from outside the school premises or school hours which reference the school or which might bring staff members or governors professional status into disrepute.*

*The school regularly reviews and updates with the assistance of the DPO, all user agreement documents to ensure that they are consistent with current school policies as listed at the end of the agreement.*

## **2. User Requirements**

*School employees, governors, and third party staff using school systems must comply with the requirements below. Failure to do so could possibly mean disciplinary procedures being started.*

*Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may be subject to monitoring.*

- a) I will only use the school's ICT resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body in the line of my employment.*
- b) I will set strong passwords, following advice provided by the school or its ICT Manager. I will change it frequently.*
- c) I will not reveal my password(s) to anyone.*
- d) I will not use anyone else's password if they reveal it to me and will advise them to change it.*
- e) I will not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system I have access to via the school or other authority or processing system.*
- f) I will ensure all documents; data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols, and retention policy.*
- g) I will not engage in any online or other media activity that may compromise my professional responsibilities.*
- h) I will only use the schools approved email system(s) for any school business.*
- i) I will only use the approved method/s of communicating with pupils or parents/carers and will only communicate with them in a professional manner and on appropriate school business.*
- j) I will not support or promote extremist organisations, messages or individuals.*

- k) *I will not give a voice or opportunity to extremist visitors with extremist views.*
- l) *I will not browse, download or send material that is considered offensive or of an extremist nature by the school.*
- m) *I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the headteacher.*
- n) *I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed. I will seek advice from the School Office and/or ICT Manager.*
- o) *I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.*
- p) *I will not connect any device (including USB flash drive), to the network 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 and other malware systems.*
- q) *I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.*
- r) *I will follow the school's policy on use of mobile phones / devices at school*
- s) *I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.*
- t) *I will only take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. I will not identify students by name, or other personal information.*
- u) *I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.*
- v) *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, and will create a distinction between the two.*
- w) *I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.*
- x) *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.*
- y) *I will only access school resources remotely (such as from home) using the school approved system and follow e-security protocols to interact with them.*
- z) *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.*
- aa) *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.*

- bb) I am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.*
- cc) I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the relevant Senior Member of Staff / Designated Safeguarding Lead.*
- dd) I understand that all internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.*
- ee) I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.*
- ff) I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.*
- gg) Staff that have a teaching role only: I will embed the school's online safety / digital literacy / counter extremism curriculum into my teaching.*

### **3. Links with Other Policies**

*I understand that this user agreement is linked to the schools:*

- *Freedom of information publication scheme*
- *Online and E-Safety Policy*
- *Email Security and Etiquette Guidance*
- *GDPR/Data Protection Policy*
- *Document Retention Policy*
- *Breach Management Policy*
- *Asset Management Recording Policy*
- *Disaster Recovery/Business Continuity Planning and Risk Register.*
- *Safeguarding and Child Protection Policy*

#### **4. Agreement Form**

##### **User Signature**

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible ICT user'.

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

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

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

Full Name ..... (printed)

Job title / Role .....

##### **Authorised Signature (Head Teacher / Deputy)**

I approve this user to be set-up on the school systems relevant to their role

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

Full Name ..... (printed)



DigiSafe



Acceptable Use Policy  
(AUP) for

**PARENTS AND CARERS**

### **What is an AUP?**

*We ask all children, young people and adults involved in the life of St Gabriel's C of E Primary School to sign an Acceptable Use\* Policy (AUP), which is a document that outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).*

*Your child has also signed an AUP. You can view our pupil AUP on our website.*

### **Why do we need an AUP?**

*These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody.*

*School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe.*

*We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community: **"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."***

### **Where can I find out more?**

*You can read St Gabriel's C of E Primary School full Online Safety Policy on our website. If you have any questions about this AUP or our approach to online safety, please speak to your child's teacher, a member of the SLT or our online safety lead, Hannah Gilbert.*

### *What am I agreeing to?*

1. I understand that St Gabriel's C of E Primary School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
6. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
7. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety (NB: the recent LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety, but only half talk about it with them more than once a year). Understanding human behaviour is more helpful than knowing how a particular app, site or game works.
8. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK.  
<https://www.internetmatters.org/>
9. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and which can be seen on the school website and I understand that s/he will be subject to sanctions if s/he does not follow these rules.

10. I can find out more about online safety at St Gabriel's C of E Primary School by reading the full Online Safety Policy found on the school website and can talk to my child's teacher, a member of the SLT or the e-safety lead if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

~~~~~

**I/we have read, understood and agreed to this policy.**

**Signature/s:**

\_\_\_\_\_

**Name/s of parent / guardian:**

\_\_\_\_\_

**Parent / guardian of:**

\_\_\_\_\_

**Date:**

\_\_\_\_\_