CHURCHFIELDS
JUNIOR SCHOOL

Online Safety Policy

October 2019

Approved by GB: October 2019

Next review due: October 2022

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and Responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation. The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1)

3.2 The Head Teacher

The Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy. The DSL takes lead responsibility for online safety in school, in particular:

- ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head Teacher, ICT Lead and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged using CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged using CPOMs and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head Teacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT Lead

The ICT Lead is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers
All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix1), and ensuring that pupils follow the school's terms on acceptable use (appendix 2)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents
Parents are expected to:

- Notify a member of staff or the Head Teacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community
Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 1).

4. Educating pupils about online Safety

Pupils will be taught about online safety as part of the curriculum.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant.
The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Pupils are taught to follow these rules:

Rules for Responsible Internet Use
The school has installed computers with internet access to help our learning. These rules will keep you safe and help us be fair to others.

- I will not access other people's files without their permission.

- I will sometimes use the computers for school work and homework.
- I will not bring in memory sticks from outside school unless I have been given permission.
- The email messages I send will be polite and responsible.
- When using the internet, I will not give my home address or telephone number, or arrange to meet someone.
- I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself.
- I understand that the school may check my computer files and may monitor the internet sites I visit.

They are also taught how to be safe online using the SMART code. See Appendix 4.

5. Educating parents about online safety

Information on responsible internet use are included in the New Entrants' Booklet. As part of the Home-School agreement, parents agree to Support the School's policies and guidelines in respect of rules, behaviour and discipline, recognising the vital role of parents in fostering good behavioural attitudes.

The New Entrants' Booklet also reminds parents to not to name or include images of any pupil or member of staff on a social media website without their permission. Failure to abide by this code could lead to more formal procedures being taken against those concerned. Parents are also reminded that social media sites are not designed for children, that children need to be 13+, and often 16+ to be using most Social Media Apps. They are reminded to check their child's phone, remove inappropriate apps, monitor online chat and texts, block children who post hurtful messages and report problems to the social media site. Online safety will also be covered if necessary during parents' evenings.

The school will also raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head Teacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the Head Teacher.

6. Cyber-bullying

6.1 Definition
Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Anti-bullying policy.)

6.2 Preventing and addressing cyber-bullying
To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
All staff and governors receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices
School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All staff, volunteers and governors are expected to agree to acceptable use of the school's ICT systems and the internet. Acceptable use is defined in the Staff Agreement Form. Acceptable use for pupils is defined in the New Entrants' Booklet, this policy and in lessons on online safety. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Break or lunch time
- Clubs before or after school, or any other activities organised by the school

Any mobile devices must be handed in to the teacher of the class in the morning. They will then be taken to the school office and collected at the end of the school day. Pupils must be told not to use the mobile device in school or on the school playground.

Any unacceptable use of mobile phones in school may result in the confiscation of their device before it is returned to a parent/carer with a meeting about the breach.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.
Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.
If staff have any concerns over the security of their device, they must seek advice from the ICT Unit.
Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT system or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. More information about safeguarding training is set out in our Child Protection and Safeguarding policy.

12. Monitoring

The behaviour and safeguarding issues related to online safety are stored on CPOMs. This policy will be reviewed by staff and governors every three years. At every review, the policy will be shared with the Governing Body. Parents are most welcome to request copies of this document and comments are invited from anyone involved in the life of the school.

Appendix 1: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors and volunteers

When using the school's ICT systems and accessing the internet in school, or outside school on a work device,

- I will not access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- I will not use them in any way which could harm the school's reputation
- I will not use access social networking sites or chat rooms, other than those currently used by the school with the purpose of monitoring or updating the school's social media feeds.
- I will not use any improper language when communicating online, including in emails or other messaging services
- I will not use install any unauthorised software
- I will not use share my password with others or log in to the school's network using someone else's details
- 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 only use the approved, secure email system(s) for any school business. This is currently LGFL Mail.
- 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 publish or distribute work that is protected by copyright.
- 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 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, and that these are secured and private.
- 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 only use LA systems in accordance with any corporate policies.
- 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.
- I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I will let the designated safeguarding lead (DSL) and ICT Lead know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I agree to abide by all the points above. 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 policies.

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

Signed (staff member/governor/volunteer/visitor):	Date:
Full name (printed)	Job Title
I approve this user to be set-up. **Authorised Signature (Head Teacher)**	Date

Appendix 2: rules for responsible use for pupils

Rules for Responsible Internet Use
The school has installed computers with internet access to help our learning. These rules will keep you safe and help us be fair to others.

- I will not access other people's files without their permission.
- I will sometimes use the computers for school work and homework.
- I will not bring in memory sticks from outside school unless I have been given permission.
- The email messages I send will be polite and responsible.
- When using the internet, I will not give my home address or telephone number, or arrange to meet someone.
- I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself.
- I understand that the school may check my computer files and may monitor the internet sites I visit.

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's rules for responsible use for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: Be SMART Online Code