STAMFORD ST GILBERT'S CHURCH OF ENGLAND PRIMARY SCHOOL

E-SAFETY POLICY

2018/19

DOCUMENT CONTROL	
Committee:	Full Board of Governors
Approved By Trustees On:	30.10.18
Review Cycle:	Annual
Date of Next Review:	September 2019

Policy Statement

This e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Safeguarding is a serious matter; at St. Gilbert's we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

This policy is available for anybody to read on the school website; upon review all members of staff will sign as having read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Pupils Acceptable Use Policy will be sent home with pupils at the beginning of each school year.

Headteacher: Frances Dicker Signed:

Chair of Governors: Signed:

Review Date: October 2018 Next Review: September 2019

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:

- Keep up to date with emerging risks and threats through technology use.
- Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

e-Safety Officer –

Working with the governing body, the e-safety Officer has overall responsibility for e-safety within our school. The day-to-day duty of e-Safety Officer is devolved to *Mrs K Standen*

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the e-safety adviser, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, is fit for purpose through liaison with the local authority and/or IT Technical Support.

ICT Technical Staff (ARK)

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
- The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the Pupil Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the school behaviour policy.

e-Safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through occasional information evenings and school newsletters posted on the school website the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that pupils are empowered.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will be notified of the student Acceptable Use Policy annually.

Governance

The Governing Body has the responsibility:

- to advise on changes to the e-safety policy.
- to establish the effectiveness and impact (or not) of e-safety training and awareness in the school.
- to recommend further initiatives for e-safety training and awareness at the school.

Technology

St. Gilbert's School uses a range of devices including PC's, iPads and laptops. In order to safeguard the pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use internet filtering software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use filtering software that prevents any infected email being sent from or received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Logins and Passwords – all staff are given a unique login and password, and access to relevant folders on the server. Staff will be reminded that passwords should be changed on a long termly basis. Pupils will only be given a unique login.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; pupils upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests; the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.
Pupils are permitted to use the school email system, and as such will be given their own email address.

Photos and videos – Digital media such as photos and videos are covered in the schools Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year as part of the permissions request form; non-return of the permission slip will be assumed as acceptance.

Social Networking – there are many social networking services available; our school is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. Social media services will be permitted for use within St. Gilbert's School and appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

Blogging and twitter will be explored in the future as an educational tool and used by staff and pupils in school.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname; first name only is to be used.
- Where blogs are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Safeguarding
In school the safeguarding of children is of utmost importance, which includes when they are using the Internet and other digital technology. As such St. Gilbert's uses filtering technology in the school, so endeavouring that no-one can get to illegal or inappropriate websites. We also have various rules and also Acceptable User Policy in place within the school for both staff and pupils to ensure their safety as much as possible. Any e-safety incidents will be reported, investigated and the findings logged after which a full report will be made to the Safeguarding Governor.
St Gilberts CE Primary School is fully committed to safeguarding and promoting the welfare of all its pupils. Every member of staff recognises that safeguarding against radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society. Our 'Tackling Extremism and Radicalisation' Policy sets out our beliefs, strategies and procedures to protect vulnerable individuals from being radicalised or exposed to extremist views, by identifying who they are and promptly providing them with support.
At our school we will promote the values of democracy, the rule of law, individual liberty, mutual respect and tolerance for those with different faiths and beliefs. We will teach and encourage pupils to respect one another and to respect and tolerate difference, especially those of a different faith or no faith. It is indeed our most

fundamental responsibility to keep our pupils safe and prepare them for life in modern multi-cultural Britain and globally.
Please refer to our Extremism and Radicalisation policy and also our Safeguarding and Child Protection Policy 2016 to understand the school's position on safeguarding all our pupils.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, St. Gilbert's School will have an annual programme of training that is in line with national requirements, is progressive and is suitable to the intended audience.

e-Safety for our pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Appendix 1

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the e-safety policy only (currently blogging). Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including email, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent of the school. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment (i.e. mobile phones, iPads etc.) is not generally permitted within school or for school business, however the Headteacher may use discretion on an individual basis.

Viruses and other malware - any virus outbreaks are to be reported to ICT Support as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with pupils.

NAME :

SIGNATURE : **DATE :**

Appendix 2

KS1/2 Charter of Good Online Behaviour

Note: All Internet and email use is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for, or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent) :

Signed (Student) :

Date :

Appendix 3

Dear Parent/Carer,

In school, the safeguarding of your children is of utmost importance, which includes when they are using the Internet and other digital technology. As such we use filtering technology in the school to ensure that no-one can get to illegal or inappropriate websites. We also have various rules in the school for both staff and pupils to ensure their safety as much as possible.

It may seem silly to suggest that when your child is at home he/she is not safe, but with the vast amount of information on the Internet, and the numerous ways to access the Internet, a whole world is potentially opened up to which you have little or no knowledge. To use an analogy, when your child plays outside you can usually see where they are and what they are doing; or at least you know where they are and what they are doing. But this isn't as easy when they are using the Internet.

One of the best ways to reduce any risk to your child is to talk to them about their online activity, and to set a few rules. In the same way as when they are playing outside they have to be in at a certain time; or if they are meeting friends you know who those friends are and where they are meeting. This instills a level of trust, and also consequences if the rules are broken.

Attached to this letter is a Contract of Good Online Behaviour. You can either use it as a guide, or you can use it as the set of rules to be hung on the wall next to the computer or gaming station. The rule should be used as a discussion point with your child to explain why the rule is in place; the promise is what your child makes. If you wish, you can make a small list of consequences like a 1 week ban if any of the rules are broken.

Appendix 4

Contract of Good Online Behaviour

Rule	Promise
I want you to enjoy the Internet but you can't be on there all the time.	I will always ask permission first and will only be on the Internet for ____ hours each night.
There are some websites and some people that want your personal information.	I will never give out personal details like my name, address, birthday, school or hobbies. If a website or somebody asks I will tell you straight away.
Like in the real world, there are some nasty people in the online world that can say or do horrible things.	If anybody is nasty to me, or says something that is hurtful, I will not talk to them. If they are a Friend I will un-Friend them. If they are on a game I am playing I will report them to the moderator. If this happens I will tell you straight away.
Friends in the online world should be like friends in the real world. Unless you know them personally you should not be talking to them.	I will never Friend anyone without asking your permission first.
Just like in the real world, you should treat people in the online world with respect.	I will always treat people with respect when online and will never bully them or say bad things.
Because of your age, there are some things that you shouldn't see.	I will tell you if I see things that I don't think I should be seeing.
Some websites and social networking sites like Facebook have age restrictions.	I will not go on websites or social networking sites if I am not old enough to be on there.
Sometimes you may hear or see things that make you feel uncomfortable.	I promise that if I ever feel uncomfortable with something I have seen or heard I will tell you straight away.

Consequences:

_____

_____

_____

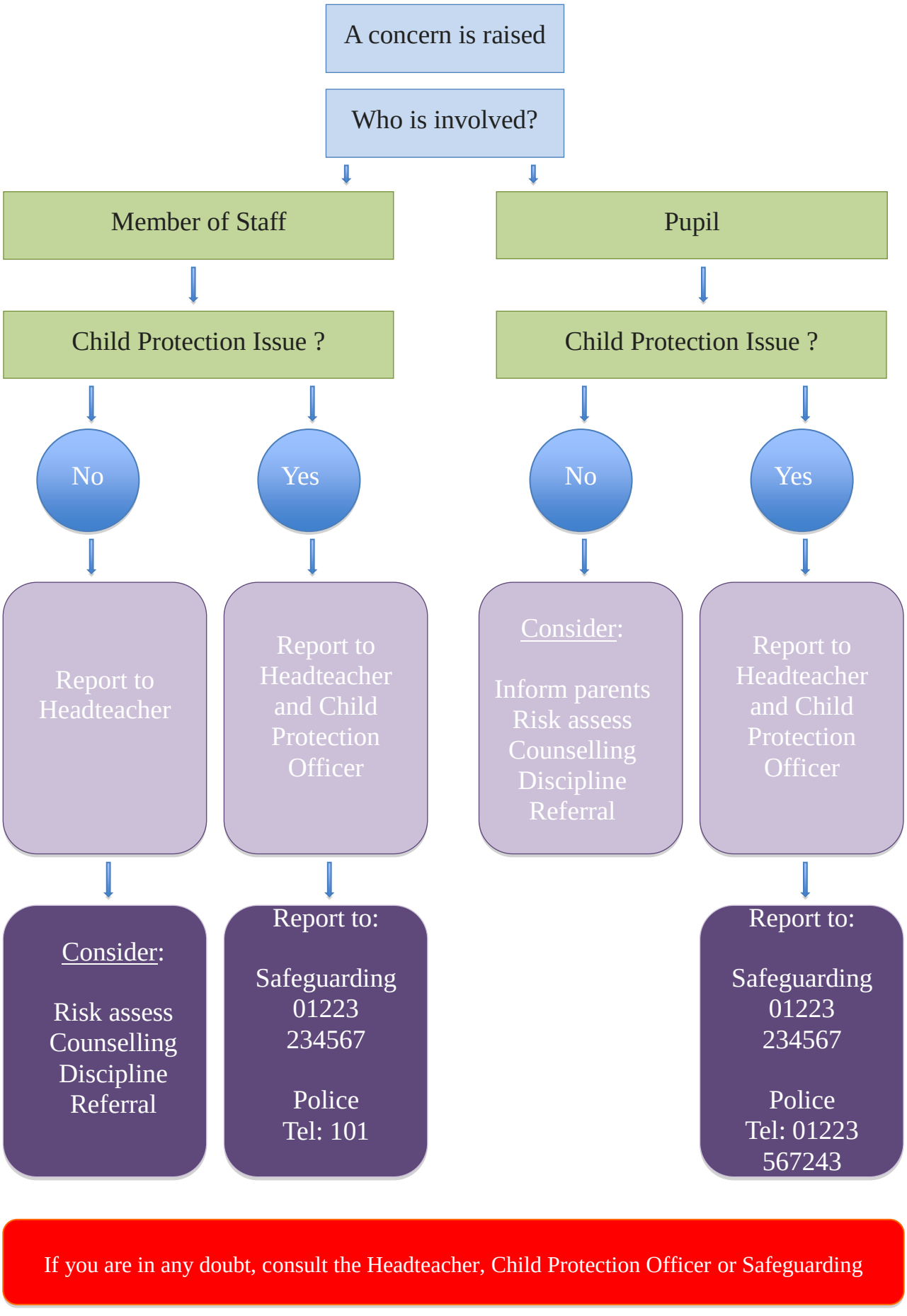
Signed: _____ Signed: _____

Appendix 5

e-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		**Date:**	
Signature (Governor)		**Date:**	

Inappropriate Activity Flowchart



If you are in any doubt, consult the Headteacher, Child Protection Officer or Safeguarding

Illegal Activity Flowchart