St Andrew's C of E School, Totteridge

e-Safety POLICY

(Non-Statutory Policy)

(Standards Committee)

(Approval by Standards Committee – 3 Year Review Cycle)

Date to be implemented from:	18th March 2021
Date to be reviewed by:	18th March 2024
Date Reviewed by Sub Committee:	2nd March 2021

Approved by:

Signed: ……. (Chair – Standards Committee)

(Print Name) …….

Date …….

This Policy supersedes any previous Policy of this name or instructions that pre-date this edition.

This Policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any pupil and it helps to promote equality at this School.

1 Policy Statement

1.1 St Andrew's School affirms that individuals are entitled to equal rights, responsibilities and opportunities. The School strives to ensure that all individuals are equally valued and everyone is treated with respect.

1.2 St Andrew's School will meet its requirement to have an e-Safety Policy as part of Data Protection/GDPR/Remote Learning and Safeguarding and meet any other legislation or requirements to ensure a safe environment for pupils, staff, parent/carers and visitors.

1.3 The Policy will be readily accessible within the School on the Website and in hard copy on request.

2 Reviewing the Policy

2.1 Reviewing the Policy – St Andrew's School will assess the implementation and impact of this Policy on a continuous basis and undertake a regular review on an annual basis to ensure it is fit for purpose.

2.2 The Policy should be read alongside the Remote Learning Policy whenever the Curriculum and wider Curriculum is being delivered to students via electronic means.

3 School Vision

3.1 Our vision is to become an outstanding School within a loving, Christian community.

3.2 Our parent/carers, children and staff will work together to enable all children to:

- achieve their potential
- learn in a safe, stimulating environment
- enjoy learning now and in the future

4 Purpose of Policy

4.1 The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to e-safety. The policy relates to other policies including Computing curriculum, Internet Access, Remote Learning, Anti-Bullying, Child Protection and Health and Safety.

4.2 It is essential that all pupils gain the confidence and ability that they need in this subject and to keep themselves safe when using all technologies both at home and at School. It is the duty of the School to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the School's physical buildings.

5 Aim of Policy

5.1 The aim of this Policy is to create a culture and ethos where all stakeholders are safe when engaging in electronic or 'virtual' activities.

5.2 St Andrews recognises that the internet/world-wide web and associated devices, such as computers, laptops, tablets, mobile phones, smartphones and games consoles are an integral part

of everyday life today and that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online and be able to identify fake information.

5.3 This Policy document is drawn up to protect all members of the School community - the pupils, parent/carers, staff, Governance and the extended members of the School community.

The Safeguarding outcomes that are applied to e-Safety includes aims that all pupils to be:

- safe from maltreatment, neglect, violence, grooming and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of School
- secure, stable and cared for

5.4 The aim is to:

- Set out the key principles expected of all members of the School community at St Andrew's with respect to the use of IT based technologies.
- Safeguard and protect the children and staff of the School.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or Codes of Practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyber-bullying and grooming cross referenced with other relevant School Policies and Procedures.
- Ensure that all members of the School community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with young children.

6 Definitions

6.1 This Policy applies to all members of St Andrew's community (including pupils, parent/carers, staff, Governance, volunteers, visitors, community users) who have access to and are users of School ICT systems, both in and out of St Andrew's premises.

6.2 The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-Safety incidents covered by this Policy, which may take place outside of the School, which is linked to membership of the School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

6.3 If an electronic device is found, a member of staff may examine any data or files on the device if they think there is good reason to do so. Following an examination, the teacher may consider that it should be returned. They may think the device should be kept or disposed of, or that images or data should be erased. To erase any data or files or confiscate a device they should consult the e-Safety leader who may consult the Headteacher, Child Protection Officer and/or Data Protection Officer as appropriate. Where there is a 'good reason' to examine or erase the data or files, staff must reasonably suspect that the data or file has been, or could be, used to cause harm, to disrupt teaching or break School rules.

6.4 The School will deal with such incidents within this Policy and associated behaviour (e.g. cyber bullying) and will, where known, inform parent/carers of incidents of inappropriate e-Safety behaviour that take place out of School.

6.5 The list below gives some examples of where risk is likely but it is not definitive. The main areas of risk for our School community can be summarised as follows:

Content

- exposure to inappropriate content (online pornography, dark web, ignoring age ratings in games, exposure to violence associated with often racist language, sexist or misogynist views, substance abuse)
- lifestyle websites (e.g. pro-anorexia/self-harm/suicide sites, gambling)
- hate sites (racist, misogynist and rape threats, trolling individuals)
- content validation (how to check authenticity and accuracy of online content)

Contact

- grooming, cyber-stalking, predators, radicalisation
- cyber-bullying in all forms, trolling
- identity theft (e.g. hacking online profiles) and sharing passwords (fraud)
- live streaming (of self-harming, sexual activity, crime, bullying)

Conduct

- privacy issues, including disclosure of personal information (hacking, phishing, spamming, scams or Trojan horse)
- digital footprint and online reputation (malicious software, malware, virus, fraud)
- posting private information and public shaming (photos, finance, locations)
- health and well-being (e.g. the amount of time spent online surfing internet or gaming)
- comparing with others (body shape, looks, embellishing the truth)
- sexting, also referred to as SGII (self-generated indecent images) sending and receiving of personally intimate images, sharing images, wearing over sexual clothing on selfies
- copyright (little care or consideration for intellectual property and ownership – such as music and film, cheating in exams or presenting other work as your own)

7 Context

7.1 The School will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a School computer or mobile device. Neither the School nor the LA can accept liability for material accessed, or any consequences of Internet access.

7.2 We use LB Barnet Computing Framework to teach e-Safety across the school community.

7.3 This Policy applies to all access to the internet and use of technology and includes personal devices when working on School work or representing the School, or where pupils, staff or other individuals have been provided with School issued devices for use off-site.

7.4 We are aware that some pupils are considered to be more vulnerable online due to a range of factors (children in care, children with SEND, children with health or mental health needs, children with EAL and children experiencing trauma or loss) and the staff will be especially vigilant to ensure that differentiated and ability appropriate on-line safety support is provided to vulnerable pupils

7.5 Our e-Safety leader acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

7.6 Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to Child Protection are dealt with in accordance with School and LA Child Protection Procedures.

7.7 Our procedures are rooted in good practice within the Curriculum. We provide a progressive e-Safety education programme as part of the computing/PSHE Curriculum. It is built on good practice from the LA, LGfL e-Safeguarding and e-literacy framework for EYFS to Y6 national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including ensuring pupils should:

- STOP and THINK before they CLICK
- develop a range of strategies to evaluate and verify information before accepting its accuracy, the veracity of content or sender of information

- always be aware that the author of a web site or page, or search engine may have a particular bias or purpose and to develop skills to recognise what that bias may be
- know how to narrow down or refine a search
- understand acceptable behaviour when using an online environment
- understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- understand that material and images you post on-line now may be detrimental many years later
- understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
- understand why they should not post or share details of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- understand why they must not post pictures or videos of others without their permission
- know not to download any files – such as music files - without permission
- have strategies for dealing with receipt of inappropriate material
- understand the impact of cyber-bullying, sexting and trolling and know how/where to seek help if they are affected by any form of online bullying
- know how to report any online/technologies abuse and how/where to seek help

8 Procedures

8.1 The e-Safety leader takes day to day responsibility for e-Safety issues and has a leading role in establishing acceptable practice and is the first line of communication for problems, information or reporting issues. Our processes are that we:

- use LB Barnet Computing Framework to teach e-Safety across the school community
- promote an awareness and commitment to e-Safeguarding throughout the school community
- ensure that e-Safety education is embedded across the curriculum
- support the e-Safety leader in delivery of training to staff and parent/carers
- inform stakeholders regarding infringements and possible sanctions
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident or breach
- ensure the e-Safety leader liaises with school IT technical staff and Data Protection Officer
- liaise with the Local Authority and relevant agencies e.g. CEOP on e-Safety
- regularly update the School on e-Safety issues and legislation

by

- monitoring the use of the network, remote access, email etc. in order that any misuse or attempted misuse can be reported immediately to the School e-Safety leader and/or Headteacher for investigation, action and sanction
- transferring data securely
- ensuring that all data held on pupils is adequately protected
- ensuring that access controls/encryption/fore walls exist to protect personal and sensitive information held on school-owned devices
- ensuring that provision exists for misuse detection and malicious attack eg. keeping anti-virus protection up to date
- applying good practice to web filtering
- informing LGfL of issues relating to the filtering applied by the Grid
- keeping up to date with technical information in order to effectively carry out the e-Safety Policy
- ensuring appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- reporting immediately any e-Safety related issues that arises

8.2 Infringements include:

Pupils

- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites
- Accessing offensive material
- Corrupting or disrupting other's data
- Cyber-bullying
- Hacking into School systems
- Stealing data or materials and presenting as their own

Staff/Adults

- Excessive use of Internet for personal activities not related to professional development
- Misuse of first level data security e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network
- Any deliberate attempt to breach GDPR/Data Protection Law or computer security rules
- Deliberately attempting to access, download and disseminate any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Using equipment or log-ins of other staff
- Encouraging or allowing children to commit an infringement with taking action

8.3 All **Staff** will:

- embed e-Safety issues in all aspects of the Curriculum and other School activities
- preview websites before use [where not previously viewed or cached] before using with pupils
- supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended, remote learning School activities if relevant)
- ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws and intellectual theft
- read, understand and help promote the school's e-Safety policies and guidance
- make clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and this should not be removed
- report any suspected misuse or problem to the e-Safety leader
- maintain an awareness of current e-Safety issues and guidance through CPD

- model safe, responsible and professional behaviours in their own use of technology
- ensure that any digital communications with parents should be on a professional level and only through School based systems, never through personal mechanisms
- file emails in a logical way, as recommended by the IT staff, so that communication 'paper' trails are kept
- report any filtering breaches to the e-Safety leader immediately
- back up as required at regular intervals
- never share log-in passwords and make them strong, change regularly
- do not use any other members of staff computer without permission and never use the log-in of anyone else

8.4 The **School Leadership** will:

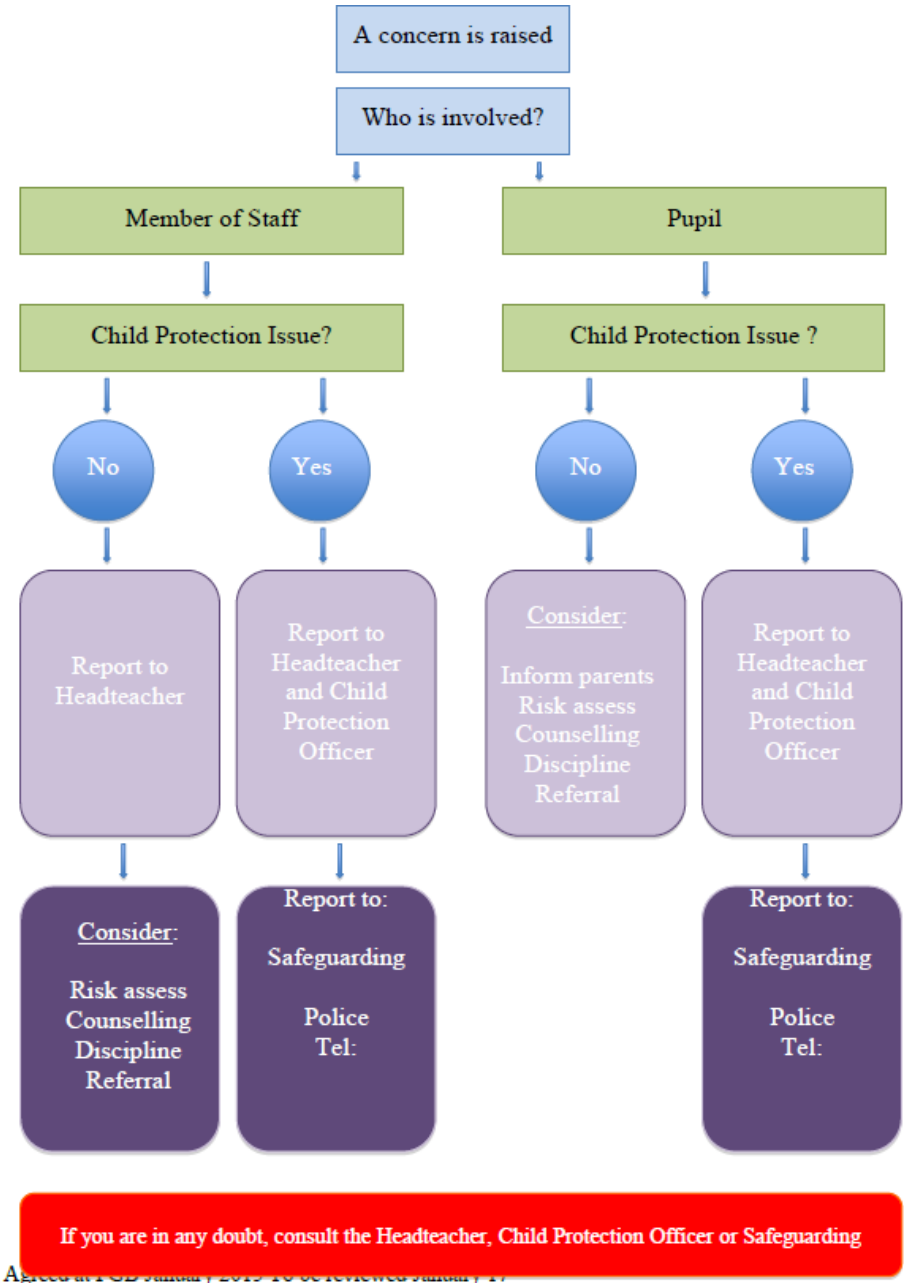
Headteacher

- ensure the Curriculum is fit for purpose and provides opportunities for the School to debate unsafe and safe practice regarding e-Safety and its implications
- take overall responsibility for data and data security as Senior Information Risk Officer (SIRO)
- liaise with the Data Protection Officer on all issues regarding data processing
- ensure that staff receive suitable training to carry out their e-Safety roles and to train other colleagues, as relevant
- ensure that there is a system in place to monitor and support staff who carry out internal e-Safety procedures (with network management)
- ensure the School uses an approved, filtered Internet Service (eg. LGfL, iCloud) which complies with current statutory requirements
- encourage parent/carers to support the School in promoting e-Safety and endorse the Acceptable Use Agreement which includes the pupils' use of the Internet and the School's use of photographic and video images
- lead the procedures to be followed in the event of a serious e-Safety incident
    - interview/counselling by class teacher, e-Safety Coordinator or Headteacher
    - inform parent/carers of investigations/issues
    - apply removal of Internet or computer access for a period
    - referral to LA / Social Services / Police in serious instances
- monitor and evaluate this Policy at regular intervals

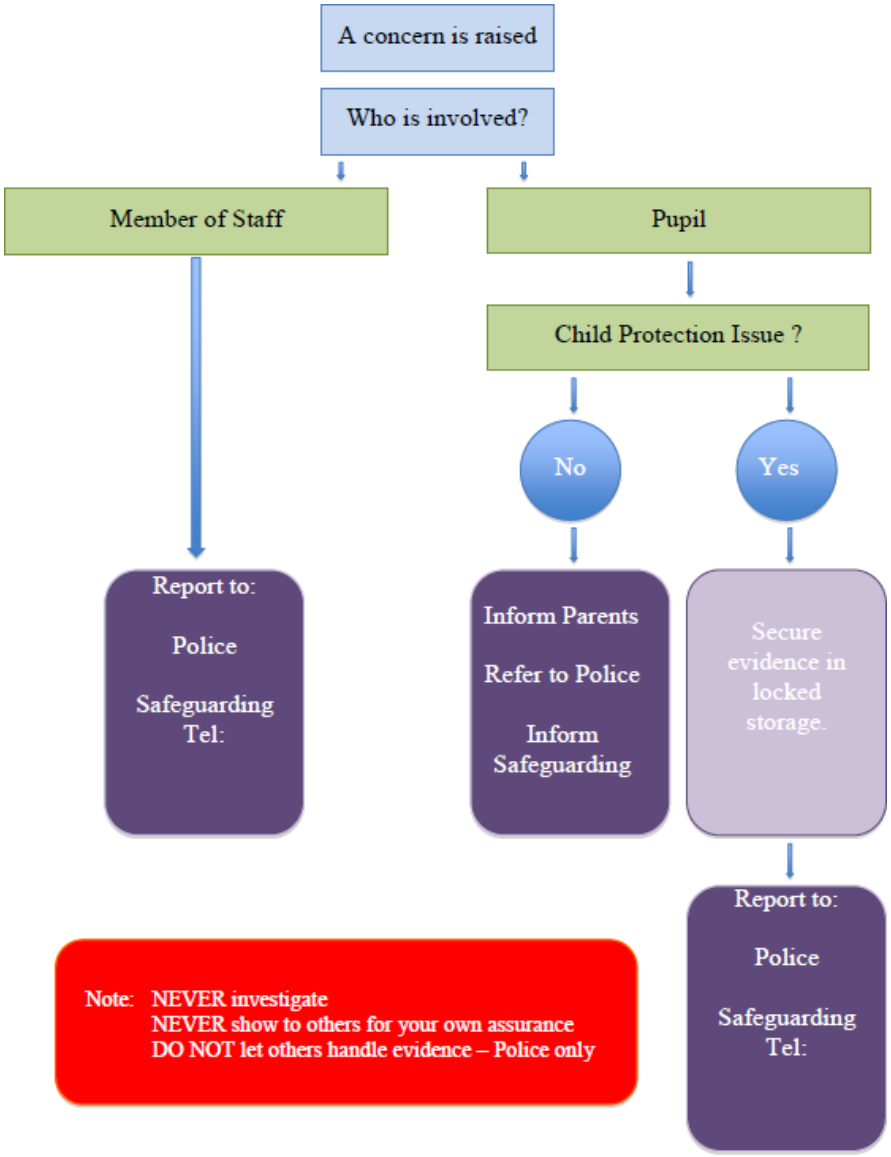
Governance

- ensure that the School follows all current e-Safety advice to keep the children and staff safe
- support the School in encouraging parent/carers and the wider community to become engaged in e-Safety activities
- ensure the named Governor for Safeguarding reports on a regular basis to the Governing Body on on-line safety incidents, including outcomes of any breaches.

APPENDIX 1 Inappropriate Activity Flowchart



APPENDIX 2 Illegal Activity Flowchart



9 Sources of further information and support

Remote Learning for Schools and Colleges - LGfL
https://www.lgfl.net/

Preparing Children to succeed in a digital world - BT
https://www.bt.com/about/digital-impact-and-sustainability/building-better-digital-lives/preparing-children-to-succeed-in-a-digital-world

Inspection, computing and e safety in schools - OfSTED

http://www.slideshare.net/Ofstednews/inspection-computing-and-e-safety-in-schools

School powers to search and screen pupils – Child law advice

https://childlawadvice.org.uk/information-pages/school-powers-to-search-and-screen-pupils/

Top 5 key cyber safety issues this school year in Australia – Family Zone

https://www.familyzone.com/anz/families/blog/five-biggest-esafety-issues