# SAFER USE OF TECHNOLOGY POLICY

## 1. INTRODUCTION

This policy takes into account the Department for Education's Advice for Parents and Carers on Cyber-bullying (November 2014) and the Department for Education's Advice on Child Internet Safety (February 2012). This policy is addressed to all pupils and parents are encouraged to read it with their child.

A copy of the policy is available to parents on request and on the School website. The School actively promotes the participation of parents to help the School safeguard the welfare of pupils and promote e-safety. This policy applies to the whole School including the Early Years Foundation Stage (EYFS).

This policy should be read in conjunction with the following:

- Child Protection Policy
- Anti-bullying Strategy
- Behaviour Policy
- Terms & Conditions
- Code of Conduct

This policy relates to e-safety and the acceptable use of technology, including:

- the internet
- e-mail
- mobile phones and smartphones/watches
- desktops, laptops, netbooks, tablets/phablets
- personal music players such as ipods
- cameras and other devices with the capability for recording and/or storing still or moving images
- social networking, micro blogging and other interactive web sites
- instant messaging (including image and video messaging via apps such as SnapChat and WhatsApp) chat rooms, blogs and message boards
- webcams, video hosting sites such as YouTube
- gaming sites
- Virtual Learning Environments such as Firefly
- SMART boards
- other photographic or electronic equipment

It applies to the use of any of the above on St. Saviour's School Ikoyi premises and also any use, whether on or off School premises, which affects the welfare of other pupils or where the culture or reputation of the School are put at risk.

## 2. AIMS

The aims of this policy are:

- to encourage pupils to make safe, secure and effective use of technology (including, but not limited to, the internet and other electronic communication);
- to safeguard and promote the welfare of pupils, in particular by anticipating and preventing the risks arising from:

a) exposure to inappropriate material (such as pornographic, racist, extremist or offensive materials);
b) the sharing of personal data, including images;
c) inappropriate online contact; and
d) cyberbullying and other forms of abuse.

- to minimise the risk of harm to the assets and reputation of the School;
- to help pupils take responsibility for their own e-safety (i.e., limiting the risks that children and young people are exposed to when using ICT)
- to ensure that pupils use ICT safely and securely and are aware of both external and peer to peer risks when using ICT;
- to prevent the unnecessary criminalisation of pupils.

## 3. SAFE USE OF ICT

The safety of pupils online is of paramount importance. Please see Appendix 1 for details of the School's e-safety procedures including:

- roles and responsibilities for the safe and acceptable use of ICT in the School;
- how the School builds resilience through education and training;
- cyberbullying - advice for pupils
- advice for parents on online safety.

## 4. INTERNET AND E-MAIL

The School provides internet access and an e-mail system to pupils to support its academic activities and to maximise the educational opportunities presented by such access. Pupils may only access the School's network when given specific permission to do so. All pupils will receive guidance on the use of the School's internet and e-mail systems.

The School's curriculum includes information about e-safety to build resilience in pupils to protect themselves and their peers. E-safety means limiting the risks that children and young people are exposed to when using technology, so that all technologies are used safely and securely.
Technology brings wonderful opportunities, not least in the classroom. St. Saviour's School Ikoyi will provide carefully-managed resources to enable children to benefit from the growing range of educational

software on the market and educate them on how to sensibly use the internet to gather information and conduct research.

Pupils are taught about general e-safety within Personal Social Health Education (PSHE), Information Communications Technology (ICT) lessons and through the annual Internet Safety day. PSHE lessons offer guidance on the safe use of social networking sites and cyberbullying whilst ICT lessons include information on blocking, removing contacts from lists, sharing of personal data and saving evidence where bullying has taken place.
For the protection of all pupils, their use of e-mail and of the internet will be monitored by the School. Pupils should remember that even when an e-mail or something that has been downloaded has been deleted, it can still be traced on the system. Pupils should not assume that files stored on servers or storage media are always private.

If a pupil is unsure about whether he/she is doing the right thing, they must seek assistance from a member of staff.

## 5. ROLE OF THE DESIGNATED SAFEGUARDING LEAD

The DSL has received training in online safety and will attend regular training on the subject. We realise that technology changes very rapidly and young people are likely to be several steps ahead of most adults. Therefore we will ensure that the DSL maintains an up-to-date awareness of the latest developments and associated risks.

Every year, during staff training in September, the area of E-Safety will be covered by an outside expert and that training will involve all staff.

## 6. SCHOOL RULES

Pupils are expected to comply with the following rules, practices and procedures:

6.1.1 E-safety (Appendix 1);

6.1.2 Internet Use and E-mail Protocol (Appendix 2);

6.1.3 Pupils mobile electronic devices (Appendix 3);

6.1.4 E-safety (Appendix 4);

6.1.5 Communication between pupils and staff (Appendix 5);

6.1.6 Guidance for Staff on Communications (Appendix 6);

6.1.7 School Policy on Safer Use of Technology (Appendix 7).

## 7. PROCEDURES

Pupils are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible during class or break time. Use of technology should be safe, responsible and legal. If a pupil is aware of misuse by other pupils, they should talk to a teacher about it as soon as possible.

Any misuse of the internet will be dealt with under the School's Behaviour Policy.

Pupils must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-bullying Strategy. If a pupil thinks that they might have been bullied or that another person is being bullied, she should talk to a teacher about it as soon as possible. See also Appendix 3 of this policy for further information about cyberbullying and e-safety, including useful resources.

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's child protection procedures as set out in the School's Child Protection Policy. If a pupil is worried about something that she has seen on the internet, she should talk to a teacher about it as soon as possible.

### Sanctions

Where a pupil breaches any of the School rules, practices or procedures set out in this policy or the appendices, the Head Teacher will apply sanctions that are appropriate and proportionate to the breach including, in the most serious cases, expulsion. Other sanctions might include increased monitoring procedures, withdrawal of the right to access to the School's internet and e-mail facilities. Any action taken will depend on the seriousness of the offence.

Unacceptable use of electronic equipment or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material in accordance with the practices and procedures in this policy and the School's Behaviour Policy.

The School reserves the right to charge a pupil or her parents for any costs incurred to the School, or to indemnify any significant liability incurred by the School, as a result of a breach of this policy.

## 8. LIABILITY OF THE SCHOOL

Unless negligent under the terms of this policy, the School accepts no responsibility to the pupil or parents caused by or arising out of a pupil's use of the internet, e-mail or any electronic device whilst at School. The School does not undertake to provide continuous internet access. E-mail and website addresses at the School may change from time to time.

## 9. REPORTING E-SAFETY ISSUES

The School reserves the right to monitor the use of the internet and email.

Staff, pupils and visitors using the School network should report any related issues and concerns to the Deputy Head Pastoral or Head Teacher. The Deputy Head Pastoral or Head Teacher will review the issue or concern, seek assistance from the IT department if required, and take any necessary action. The member of staff, pupil or visitor raising the concern or issue will be kept informed of developments and any action taken as a result.

All serious e-safety incidents should be reported to the Head Teacher and will be recorded in the Discipline Log.

## 10. MONITORING AND REVIEW

The Head Teacher is responsible for the implementation and annual review of this policy, and will consider the record of e-safety incidents and new technologies where appropriate, to consider whether existing security and e-safety practices and procedures are adequate. This policy will be reviewed more frequently if changes to legislation, regulation or statutory guidance so require.

| | |
|---|---|
| Policy established and agreed: | January 2018 |
| Policy review cycle: | Annual |
| Policy reviewed: | Lent 2020 |
| Date of next review: | Lent 2021 |
| Member of staff responsible for the policy: | Mr Craig Heaton (Head Teacher) |

## Appendix 1: E-Safety

The School is committed to safeguarding the welfare of all pupils and an effective e-safety strategy is paramount to this.

### ROLES AND RESPONSIBILITIES

### The Board of Management

The Board of Management has overall responsibility for the safeguarding procedures within the School, the day to day responsibilities for which are delegated to the Head Teacher. The Nominated Safeguarding Governor takes leadership of the School's safeguarding arrangements, including the School's online safety procedures, on behalf of the Board of Management

The Board of Management will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of how pupils may be taught about safeguarding, including online safety, through the School's curricular provision, ensuring relevance, breadth and progression.

### Head and Senior Leadership Team

The Head Teacher has overall responsibility for the safety and welfare of members of the School community. The Head Teacher delegates day to day responsibility for the online safety of pupils to the Designated Safeguarding Leads as the persons with responsibility for safeguarding in the School.

The Designated Safeguarding Leads are responsible for managing online safety incidents in the same way as other safeguarding matters in accordance with the School's Child Protection Policy and procedures including the keeping and monitoring of the Discipline Log.

The Designated Safeguarding Leads will work with the IT department (see below) in monitoring the School's IT safety practices and the implementation of the procedures to assess whether any improvements can be made to ensure the online safety and wellbeing of pupils.

The Senior Leadership Team will be updated regularly by the Designated Safeguarding Leads on the operation of the School's safeguarding arrangements, including online safety practices.

### IT Department

The IT Department is responsible for the operation of the School's filtering system to ensure that pupils are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network. The School will do all it reasonably can to limit pupils exposure to the aforementioned risks when using the School's IT systems by utilising the filtering system to safeguard pupils

from potentially harmful and inappropriate material online without "over blocking" or imposing unreasonable restrictions as to what pupils can be taught through online teaching.

The IT Department is responsible for ensuring:

- that the School's technical infrastructure is secure and is not open to misuse or malicious attack;
- that users may only access the School's networks and devices if properly authenticated and authorised;
- that the filtering policy is applied and updated on a regular basis;

The School's current monitoring system is able to highlight misuse of the IT system. The IT Department will immediately report the issue to the Deputy Head and Head Teacher. All safeguarding concerns must be immediately reported to the Designated Safeguarding Leads.

### All staff

The School's staff have a responsibility to act as good role models in their use of technologies, the internet and mobile electronic devices.
Staff are expected to comply with the separate policies which forms part of their contract of employment.
Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Child Protection Policy and procedures.

### Education and training

Internet safety is integral to the School's ICT curriculum. The safe use of ICT is also a focus in all areas of the curriculum and key ICT safety messages are reinforced as part of assemblies and tutorial/ pastoral activities, teaching pupils:

- about the risks associated with using the internet and how to protect themselves and their peers from potential risks;
- to be critically aware of content they access online and guided to validate accuracy of information;
- how to recognise suspicious, bullying or extremist behaviour;
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- the consequences of negative online behaviour; and
- how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly;

The School provides e-safety training to staff to protect pupils and themselves from online risks and to deal appropriately with e-safety incidents when they occur.
Ongoing staff development training includes training on online safety together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements.

## Appendix 2 Internet Use and E-mail Protocol

### Introduction

We want each pupil to enjoy using the internet, and to become proficient in drawing upon it both during their time at School, and as a foundation for their further education and career. However, there are some potential drawbacks with e-mail and the internet, both for pupils and for the School.

The purpose of these rules are to set out the principles which pupils must bear in mind at all times and also the rules which must be followed in order for all pupils to use the internet safely and securely.

The principles and rules set out below apply to all use of the internet, including social media, and to the use of e-mail in as much as they are relevant. Failure to follow these rules will constitute a breach of discipline and will be dealt with in accordance with the School's Behaviour Policy.

### Access and security

Computer facilities are provided within the school to allow pupils to extend their ICT skills and to use as a tool in all curriculum subjects to research, analyse, exchange and present information. Priority is always given to educational activities over private use.

If there is a problem with passwords, pupils must approach the ICT Teacher, in person, for assistance. The ICT Teacher will speak to the IT department before resetting a pupil's password.

Pupils must log off or lock their workstations if they leave the workstations for any period of time.

Pupils must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the School's or any other computer system, or any information contained on such a system.

The School has a firewall in place to ensure the safety and security of the School's networks.
Pupils must not attempt to disable, defeat or circumvent any of the School's security facilities. Any problems with the firewall must be reported to the class teacher or the IT Department. The School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils.

Viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to e-mails. If a pupil thinks or suspects that an attachment, or other material to download, might contain a virus, she must speak to her class teacher and/or the IT department before opening the attachment or downloading the material. Pupils must not disable or uninstall any anti-virus software on the School's computers.

## Use of the internet

Pupils are permitted to use the School's computer systems for personal or leisure use however, priority must always be given to someone with school work to do.

Pupils must take care to protect personal and confidential information about themselves and others when using the internet, even if information is received or obtained inadvertently.

Pupils should not put personal information about themselves, for example their full name, address, date of birth or mobile number, online. Receiving or using this kind of information may be unlawful under data protection legislation and laws relating to confidentiality.

Pupils should assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights - pupils must not copy (plagiarise) another's work.

Pupils must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of ICT in this way is a serious breach of discipline. Pupils must tell a member of staff immediately if they have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

Pupils should not enter into any contractual commitment using the internet when in the care of the School, or otherwise associated with the School, whether for themselves or on behalf of another (including the School).

Pupils must not bring the School into disrepute through their use of the internet.

## Use of e-mail

E-mail should be treated in the same way as any other form of written communication. Pupils should not include or ask to receive anything in an e-mail which is not appropriate to be published generally or which the pupil believes the Deputy Head or Head Teacher, and/or their parents would consider to be inappropriate.

Pupils must not send, search for or (as far as pupils are able) receive any e-mail message which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of a terrorist related nature, sexist, homophobic, any form of bullying, religious extremism, pornographic, defamatory or criminal activity. If pupils are unsure about the content of a message, they must speak to a member of staff. If a pupil comes across such material she must inform a

member of staff as soon as possible. Use of the e-mail system in this way is a serious breach of discipline. The School will take no responsibility for any offence caused by a pupil as a result of downloading, viewing or forwarding inappropriate e-mails.

Trivial messages and jokes should not be sent or forwarded through the School's e-mail system. Not only could these cause distress to recipients (if inappropriate) but could also cause the School's ICT system to suffer delays and/or damage. Pupils must not read anyone else's e-mails without their consent.

## Appendix 3 Pupils mobile electronic devices

### Use of mobile electronic devices

"Mobile electronic device" includes without limitation mobile phones, smartphones/watches, tablets, laptops. We operate a no mobile phone policy.

In emergencies, pupils may request to use the School telephone. Parents wishing to contact their children in an emergency should always telephone the School office and a message will be relayed promptly.

Pupils may not bring mobile electronic devices into School except where special arrangements for the use of a tablet or laptop have been agreed with the Head.

Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline, whether or not the pupil is in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the School's Anti-Bullying Strategy and Behaviour Policy).

The School reserves the right to confiscate a pupil's mobile electronic device for a specified period of time if the pupil is found to be in breach of these rules.

The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed in to staff.

### Photographs and images

Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

Pupils may only use cameras or any mobile electronic device with the capability for recording and/or storing still or moving images with the express permission of the member of staff in charge and with the permission of those appearing in the image.

All pupils must allow staff access to images stored on mobile phone and/or cameras and must delete images if requested to do so.

The posting of images which in the reasonable opinion of the Head Teacher, is considered to be offensive on any form of social media or websites such as YouTube etc. is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

Pupils are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the School and may constitute a criminal offence. The School will treat incidences of sexting (both sending and receiving) as a safeguarding matter under the School's child protection procedures. Pupils concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

Mobile electronic devices will be confiscated and searched in appropriate circumstances. Please see the School's Behaviour Policy on the searching of electronic devices.

## Appendix 4: E-Safety

### The School's responsibilities include:

- focusing on e-safety in all areas of the curriculum and reinforcing key e-safety messages as part of assemblies and tutorial/pastoral activities, teaching pupils:
- about the risks associated with using the internet and how to protect themselves from potential risks;
- to be critically aware of content they access online and guided to validate accuracy of information;
- how to recognise suspicious or bullying behaviour;
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- the consequences of negative online behaviour; and
- how to report cyberbullying and/or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly;
- ensuring that the School's staff act as good role models in their use of technologies, the internet and mobile electronic devices;
- providing staff with online training in e-safety which enables them to identify online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on Educare for a number of courses including e-safety;
- logging and monitoring e-safety incidents and regularly reviewing this policy to ensure that the School's e-safety practices and procedures are adequate.

### Cyberbullying

Cyberbullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature:

Pupils should remember the following:

- Always respect others - be careful what you say online and what images you send.

- Think before you send - whatever you send can be made public very quickly and could stay online forever. If you or someone you know are being cyberbullied, TELL SOMEONE. You have the right not to be harassed or bullied online. Tell an adult you trust - your parents or any member of staff

- Do not retaliate or reply online.

- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the School to investigate the matter.

- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.

- If you see cyberbullying going on, support the victim and report the bullying.

Any incident of cyberbullying will be dealt with in accordance with the School's Anti-bullying Strategy.

## Parents

The role of parents in ensuring that pupils understand how to stay safe online is crucial. The School expects parents to promote e-safety and to:

- support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;

- talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

- encourage their child to speak to someone if they are being bullied or need support.

If parents have any concerns or require any information about e-safety, they should contact the Designated Safeguarding Leads.

## Useful resources for pupils and parents

http://www.childnet.com http://www.saferinternet.org.uk http://www.kidsmart.org.uk

http://www.safetynetkids.org.uk http://www.safekids.com http://www.thinkuknow.co.uk

DfE's Advice for Parents and Carers on Cyberbullying

http://parentinfo.org

DfE's Advice on the use of social media for online radicalisation

## Appendix 5 Communication between pupils and staff

The School is committed to safeguarding and promoting the welfare of children at the School and we therefore expect pupils and staff, and where appropriate, parents, to follow these rules on communication by mobile phone, tablet or similar device. Pupils must use their School email accounts for any email communication with staff. Communication either from a pupil's personal email account or to a member of staff's personal email account is not permitted.

Pupils should avoid using mobile phones to speak to or send messages to staff whilst in or out of School. Telephone numbers should not be exchanged or displayed. Any messages that are sent should be brief and courteous. Pupils must not access or use social networking sites of members of staff.

### Educational Visits

The leader of an educational visit will carry a mobile phone supplied by the School and, as part of the preparations for the visit, will ensure that relevant numbers are exchanged with pupils and other adults taking part in the visit.

Pupils taking part in such visits should avoid using mobile phones to speak to or send messages to staff except in emergencies. Any messages that are sent should be brief and courteous.

### Inappropriate communications

If there are reasonable grounds to believe that inappropriate communications have taken place, the School will require the relevant mobile phones to be produced for examination. The usual disciplinary procedures will apply. Pupils may expect to have mobile phones confiscated if there has been a breach of these rules.

## Appendix 6: Guidance for Staff on Communications

All communication with pupils or parents should conform to School policy and be limited to professional matters. Except in an emergency, communication should only be made using School property.

Communication from a member of staff's personal email account to a pupil's personal email account is not permitted.

As a general rule members of staff who receive communications to their School email account, from a pupil's personal email account, should redirect their response to the pupil's School email account, unless it is not possible to do so for technical reasons. If a member of staff has any concerns about a pupil using their personal email account to contact them the member of staff should raise their concerns with the Designated Safeguarding Leads.

Staff must not access or use social networking sites of pupils, or use internet or web-based communication channels to send personal messages to pupils. Staff must ensure their personal social networking sites are set as private and pupils are not approved contacts.

Staff should not give their personal contact details, including e-mail addresses, home or mobile telephone numbers etc. to pupils unless the need to do so is agreed beforehand with the Head Teacher and parents, guardians or carers.

E-mail or text communications between staff and pupils outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through the internet or web-based communication channels.

## Appendix 7 School Pupil Policy on the Safer Use of Technology

When using technology at School, I will stay SAFE.

| | | |
|---|---|---|
| S |  | I will only use the Internet and email with an adult. |
| A |  | I will only click on icons and links when I know they are safe. |
| F |  | I will only send friendly and polite messages. |
| E |  | If I see something I don't like on a screen, I will always tell an adult. |

My Name: _____

Parent's signature: _____

Date : _____