ST AIDAN'S
Voluntary Controlled
PRIMARY SCHOOL
Albany Road
London N4 4RR
T: 020 8340 2352
F: 020 8341 2320
E: admin@staidansprimaryschool.org.uk
W:www.staidansprimaryschool.org.uk
Headteacher: Anne Etchells

E-safety policy

Introduction

At St Aidan's we have a diverse, balanced and creative approach to employing electronic technology across most subject areas but we are acutely aware of the potential problems children can find themselves in. We ensure all our staff and children understand these risks and know how to avoid them. All pupils are taught about e-safety and staff are committed to keeping this important subject a topical issue.

Contents

1 Aims and objectives

The aim of this policy is to protect everyone involved in the school from being a participant in or the victim of, illegal, offensive or harmful activities associated with modern electronic media.

1.1 This policy lays out the acceptable use of computers, cameras, mobile phones and other portable devices in a way that can be understood and adhered to by everyone involved in the school. (See also our *GDPR policy*.)

1.2 Failure to comply with this policy may lead to disciplinary procedures.

1.3 To promote the aims of this policy we hold an e-safety assembly for the children each term. The same information is conveyed to parents and carers in our newsletter and while they are gathered prior to the Friday class assemblies. Regular reminders about e-safety in the home are also provided through our newsletter and website.

2 Definitions

2.1 Portable devices include smartphones, tablets, laptops and mp3 players.

2.2 Social networking sites are those such as Facebook, Youtube, Twitter, Snapchat, RoadBlox etc.

2.3 Within this policy we define illegal or inappropriate content as:

- Pornography or indecent images;
- films showing 'happy-slapping'/bullying/substance abuse;
- text messages or posts that contain offensive or bullying language or images;
- any age inappropriate material.

3 Electronic communication with the school

3.1 Children do not have school email addresses.

3.2 Teachers have school email addresses which are only used for internal communication.

- If parents wish to email queries they should do so to the school administrator (admin@staidansprimaryschool.org.uk) who will confidentially pass them on to the appropriate member of staff.

3.3 Each year group has a dedicated school email address for general communication about children's work.

3.4 Most parents are signed up to our text messaging service which is frequently used to distribute information.

3.5 In order to reduce paper usage, we are moving towards email communication wherever possible: general information, including the Headteacher's fortnightly newsletter, *Headlines*, is now emailed to parents as are homework and curriculum booklets. Paper will continue to be used only where return slips are required or recipients have no access to the internet.

3.6 We publish a lot of information on our website (www.staidansprimaryschool.org.uk) and we aim to keep this updated regularly. Information such as policy documents and *Headlines*, can be downloaded as PDFs.

3.7 We do not communicate via social networking sites.

4 Servers, passwords and data security

The licensed software we use for administration and the filtering systems we use to block viruses and inappropriate material are security checked and approved by LGfL (London Grid for Learning).

4.1 Some websites and servers require passwords when logging on. Children are taught the importance of always keeping these strictly to themselves.

4.2 There are three servers at the school, each with increasing levels of restriction:
a. a pupil server for which all children and staff have passwords;
b. a teacher server for which staff only have passwords;
c. an administration server, restricted to the administrators and Senior Leadership Team.

4.3 All teachers have passwords to the external LGfL server giving access to a wide range of services.

4.4 All teachers regularly change the passwords they use to access the school network to ensure security.

4.5 Children automatically have LGFL email addresses, which, together with their log-ins, give them the potential to access individual blogs and LGFL content from home and school to work on specific fixed-term projects.

4.6 Supply teachers and other visiting teachers are given a dedicated password that allows them to use our software without compromising security of our servers.

4.7 Data is held securely and is handled sensitively and appropriately. Our servers are automatically backed up every week onto an external hard drive which is stored in a fire-proof safe.
- All school business is conducted through secure LGFL email accounts.
- All teachers have password protected USB keys for transporting teaching materials and documents. Keys must be returned to the Headteacher when a staff member leaves the school.
- When working on documents containing sensitive information (eg. reports or LSPs) on classroom computers, teachers must ensure their displays are set to computer only.
- Teachers must not download students' personal data onto their own computers.

4.8 Any data breaches must be reported to the Headteacher and Data Protection Officer.

5 Working online

Children are supervised at all times, including break times, when working online.

5.1 In the unlikely event that any inappropriate material slips past our filtering system, children are taught to report it immediately to a member of staff. The lead teacher for Computing (who keeps a record of all such incidents) and the Designated Safeguarding Lead will be informed and the site will be blocked manually. Inappropriate content is reported to Apple/Google.

5.2 School employees may be given the same limited access to our Wi-Fi network as supply teachers.

6 Photographs and videos

As part of the home school agreement we seek permission for the use of photographs and videos of children on our website, in newsletters and other publications. These forms are signed on entry to the school. Parents who change their minds about permitting publishing privileges should inform the school in writing. All staff are aware of the list of children for whom we do not have such permission.

6.1 Photographs and videos of children are not published on sites other than the school's own website without express permission from the Headteacher.

6.2 It is essential that all photographs are deemed suitable – great care must be taken not to make children feel uncomfortable or embarrassed; pictures of children in toilets or undressing are forbidden.

6.3 If we caption children in photographs we only ever identify them by their first names.

6.4 The school's cameras should be used to record school events, trips, classroom activities and work. Photography must be carried out either by, or under the supervision of, the designated member of staff.

6.5 All cameras are kept in secure lockers in the office and are put back at the end of every session.

6.6 Pictures taken and stored on the camera should be downloaded on to a school server as soon as possible.

6.7 School memory cards must not be used in other cameras: they should only be used in the camera to which they are assigned and the class teacher's desktop computer. They should be wiped at the end of each term.

6.8 Photographs of all our staff and governors are published on our website and noticeboards with their permission.

6.9 CCTV is used at the front gate, the outside area, and in the Computing room. CCTV footage is recorded and kept for security purposes only.

6.10 At St Aidan's we have no wish to prevent parents or carers taking photographs or films of the children in our care. We cannot, however, give permission for their publication. It is essential, therefore, that permission is obtained from the parents of all children appearing in images that are to be, for example, uploaded to the internet.

7 Mobile phones and other portable devices

7.1 Staff at St Aidan's may bring in mobile phones or other portable devices for their own use but may only use them during breaks or non-contact time. At all other times these must remain switched off and be kept in a locker or bag. Other adults visiting during school hours are asked to comply with this rule.

7.2 If a member of staff has a family emergency they may either seek permission from the Headteacher to keep their mobile phone to hand or they may use the school's or their own phone to make calls from the staff room or the school office..

7.3 The school has a number of mobile phones for use during school trips as staff are not to use their personal phones to contact parents. Parents attending these trips must not use their personal mobile phones when with the children.

7.4 Staff must not use their mobile phones either to contact current pupils or store their telephone numbers and personal details on them except in exceptional circumstances. In such cases the express permission of the Headteacher is required.

7.5 Children are not allowed their personal mobile phones or other portable devices at school. If any such device is brought into school it must be left in the office in the morning and may only be collected in the afternoon at the end of the school day.

7.6 Tablet computers are widely used in school. The children are supervised when using portable devices that can access the internet. The same LGfL filtering system ensures safe, appropriate content.

7.7 It is absolutely forbidden to bring any portable device into school containing inappropriate or illegal material.

8 Social media and online discussion

Children do not have unsupervised access to these sites at school.

8.1 All staff at St Aidan's are strictly prohibited from:

- publishing, viewing or commenting via any form of social media during work hours or from the school's facilities;
- disclosing any information regarding children or staff (written or pictorial), and other confidential information regarding the school, even in private messages to other members of staff;
- using the school's name for social media identities, log-in IDs and user names without prior approval from the Headteacher;
- using the school's logo on any internet posting unless they are doing so on behalf of the school with clear permission from the Headteacher or Chair of Governors.

8.2 When engaging in online discussions, staff are expected to

- make it clear that the opinions and views expressed are solely those of the author and do not necessarily represent the views of the school management or other staff;

- always exercise good judgement and common sense regardless of whether online comments relate to their job;
- respect copyright, privacy, fair use and other applicable laws.

8.3 Staff must not post comments that can be interpreted as:
- illegal activity;
- offensive, personal attack or defamation;
- bullying and harassment;
- Spam.

9 Dealing with infringements

It is the responsibility of all members of staff to be vigilant and report any concerns they might have to the Headteacher.

9.1 All concerns will be taken seriously, logged and investigated appropriately. Instances where the school is brought into disrepute may constitute misconduct or gross misconduct and disciplinary action may be applied (using the LA Disciplinary procedure).

9.2 Should there be any cause for concern, the Headteacher reserves the right to check images or other content stored on a mobile phone or other portable device belonging to a member of staff.

9.3 The Designated Safeguarding Lead will be informed immediately if any inappropriate material is discovered and the LA will be contacted for advice about how to deal with it.

9.4 Any incident where inappropriate material might have been seen by a child at school must be reported to the class teacher, lead teacher for Computing, Designated Safeguarding Lead and Headteacher.

9.5 We encourage children to discuss any anxieties they may have regarding inappropriate material they have seen outside school.

9.6 The school provides advice to parents on the use of child friendly filters.

10 Training

E-safety is an extremely important aspect of child protection. Governors and staff are given regular child protection updates and reminders of e-safety procedures throughout the year. E-safety is also raised at staff meetings whenever new issues come up.

10.1 All staff have regular training in the General Data Protection Regulation (GDPR) to ensure they are kept fully up-to-date.

11 Responsibilities, monitoring and review

11.1 The Care and Communication committee is responsible for the creation of this policy and its annual review.

11.2 The Headteacher is responsible for ensuring that:

- this policy is implemented;
- e-safety is included in the Child Protection training;
- staff are fully trained in E-safety and the GDPR..

11.3 The lead teacher for Computing is responsible for monitoring the effectiveness of this policy and ensuring that:

- the filtering systems are robust:
- the incident log is monitored;
- e-safety is taught regularly to all children.

12 Glossary

blog	Simple website
CCTV	Closed circuit television
download	put material onto a computer
GDPR	General Data Protection Regulation
LA	Local authority
LGFL	London Grid for Learning
online	connected to the internet
PDF	Portable document format
upload	put material onto a website or blog
USB stick	Small device for transferring digital material
Wi-Fi	Wireless connection

Date of policy: JUNE 2020

Policy ratified: …….. (Signature) …… (Date)

Review due: JUNE 2021