ST DUNSTAN’S, CHEAM, C of E PRIMARY SCHOOL

Policy Subject: E-SAFETY

Date: February 2019
Review: February 2021 – or before if new updates given

Mission Statement

‘St Dunstan’s - excellence in Christian education’

Our School fosters a Christian ethos and provides a high quality of care and education for every member of the school community. Christian values are promoted through the whole curriculum. We aim to motivate everyone to engage fully in the broad range of educational opportunities provided to develop their potential.

We encourage all our children to achieve high standards and to grow as happy, confident, compassionate, independent young people who show respect for others, have a desire to learn and who are eager to make positive and caring contributions to the wider community, its people and environment

RATIONALE

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management information systems.
This e-safety policy considers the use of both fixed and mobile Internet, PCs, laptops, webcams, digital video equipment, mobile phones, camera phones, personal digital assistants and portable media players. It will be revised to incorporate new and emerging technologies. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the ICT coordinator before use in school is allowed.
The school will ensure that all members of the school community are aware of the e-safety policy and the implications for the individual. E-safety depends on staff, governors, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies.

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

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.

Internet use will enhance learning:

Instruction in responsible and safe use by pupils will precede Internet access. As part of the curriculum, pupils will be made aware of the guidelines for the acceptable use of the Internet and what is not acceptable. These guidelines for acceptable use will be clearly on display in all areas of the school where Internet access is available. All pupils will be given clear objectives when using the Internet. Where Internet activities are part of the curriculum they will be planned so that they enrich and extend the learning activities. Staff will guide pupils through on-line activities that will support the learning outcomes planned for the age and maturity of the pupils. All websites used for specific activities will have been approved by the school.

Curriculum activities that involve the use of the Internet for gathering information and resources will develop pupil skills in locating and evaluating materials.

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

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

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

Pupils will be taught how to evaluate Internet content:

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board 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).

The safeguarding governor is Mrs Nikee Cristie.

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 2)

The headteacher

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

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:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on the school's pink 'Concern' forms and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged 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 headteacher and/or governing board

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher 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 1)

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

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 2).

Managing Internet Access:

Internet access in the school is provided via a broadband link through the Cygnet ~~Swan~~ Portal intranet. Filtering appropriate to the age of the pupils is provided as part of this link. An agreement for the provision of a suitable virus protection system has been implemented through the services of Cygnet IT Services, who monitor and service the school network. This virus protection system is installed on all computers in school and automatically updated regularly. Laptops will only be updated for viruses when they are connected to the network. Children are not permitted to use personal music players, digital cameras, camera phones or any other electronic device in school. Pupil access to the Internet will be by adult demonstration or directly supervised access to specific, approved on-line materials.

Children in Year 6, and those who walk to school in Year 5 are permitted to bring mobile phones to school, but they are to be handed to the class teacher (who will lock them away) at the beginning of the school day and collected at home time. The use of mobile phones will not be permitted during lessons or during the school day. Other year groups may only bring in their phones by individual consent from the head teacher and for exceptional circumstances stated clearly in writing by parents.

E-mail:

Curriculum activities that involve the use of e-mail will be through the use of individual webmail accounts that are controlled by Management Information Services. All e-mail communications sent by members of staff that relate to the school will be through authorised, MIS webmail accounts, except in exceptional circumstances. The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.

Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.

Online chat rooms and instant messaging services are blocked by the intranet filtering.

Published content and the school website:

The contact details on the website should be the school address, e-mail and telephone number.

Staff or pupils' personal information will not be published.

Publishing pupil's images and work:

Photographs that include pupils will be selected carefully and will only feature pupils with parental permission.

Only first names of pupils will be published and these will never be published in conjunction with photographs.

School newsletters are published fortnightly on the school website, but full names are never published alongside photographs of the relevant children.

Social networking and personal publishing:

The school will block access to social networking sites.

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering:

If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator immediately.

Procedures for Whole School Authorising Internet access:

A consent form, which covers permission to access the Internet, will be issued to parents and carers of each year group at the start of the academic year as part of the annual 'Overview' meetings cover the forthcoming academic year. This will contain the acceptable use guidelines and details of the school e-safety policy. Parents and carers will be required to sign the consent form and where appropriate pupils will also be required to sign an acceptance of both the acceptable use guidelines and the e-safety policy (appendix 1).

Parents of children who arrive mid-year will also be asked to sign this as part of their induction routine. The signed consent form must be returned to the school for pupil access to the internet to be permitted.

Pupils will be informed that Internet use will be monitored. Pupil access may be withdrawn if the acceptable use guidelines are not adhered to.

All members of staff including teachers, supply staff, teaching assistants and support staff, will be provided with access to a copy of the school e-safety policy.

All staff will need to sign a copy of the Staff Acceptable Use Policy before using any Internet resource in school. (Appendix 2) Staff will be made aware that Internet traffic can be monitored and traced to the individual user and professional conduct is essential.

At EYFS, access to the Internet will be by adult demonstration with occasional directly supervised access to specific approved on-line materials.

Assessing risks:

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access. Any pupil who discovers such material must immediately report it to a member of staff.

The school will audit Computing provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-Safety complaints:

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the head teacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

E-Safety Communications:

Introducing the e-Safety policy to pupils:

E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.

Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy:

All staff will be given the School e-Safety Policy and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support:

Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school website. E-safety briefings for parents will also be provided biennially or as required.

Failure to comply:

Where incidents occur due to non-compliance with the school e-safety policy these will be reported to a delegated senior member of staff. Any issues relating to staff misuse must be referred to the head teacher.

Should it become necessary to prohibit the use of Internet resources for a pupil then parents or carers will be involved so that a partnership approach can be used to resolve any issues.

This could include practical sessions and suggestions for safe Internet use at home.

Educating parents about online safety

The school will 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 headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

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 school behaviour policy.)

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, 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, governors and volunteers (where appropriate) 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.

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.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet (appendices 1 and 2). 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.

More information is set out in the acceptable use agreements in appendices 1 and 2.

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 2.

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 manager.

Work devices must be used solely for work activities.

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 systems 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.

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, every year. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors may receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log be found in appendix 4 and is kept securely in the monitoring file along with all safeguarding information in the Head Teacher’s office.
This policy will be reviewed every two years by the DSL or when new updates are given. At every review, the policy will be shared with the governing board.

Links with other policies

This e-safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable Use Agreement

Appendix 1

ST DUNSTAN’S, CHEAM, C of E PRIMARY SCHOOL

Pupil Acceptable Use Policy

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school’s computers for schoolwork, homework and as directed.
2. I will not bring files into school (on removable media or online) without permission or upload inappropriate material to my workspace.
   I will only edit or delete my own files and not view, or change, other people’s files without their permission.
3. I will keep my logins, IDs and passwords secret.
4. I will use the Internet responsibly and will not visit websites I know to be banned by the school or visit any website that I know to be inappropriate either by age limit or content. I am also aware that during lessons I should only visit websites that are appropriate for my studies.
5. I will only e-mail people I know, or those approved by my teachers.
6. The messages I send, or information I upload, will always be polite and sensible.
7. I will not open attachments, or download a file, unless I have permission or I know and trust the person that has sent them.
8. I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
9. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
10. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a teacher / trusted adult.
11. I am aware that some websites and social networks have age restrictions and I should respect this.
12. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself or other persons at risk.
13. I am aware that if I use any personal device whilst at school which causes harm, breaks school rules or disrupts teaching, then the device can be confiscated by a teacher and my parents will be informed.

I have read and understand these rules and agree to them.

Name: ***Class/Yr:***

Signed: ***Date:***

Appendix 2

ST DUNSTAN’S, CHEAM, C of E PRIMARY SCHOOL

Adult Acceptable Use Policy

In this school community, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s E-Safety Policy covers their actions out of school, if related to their membership of the school.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child’s entry to the school.
- Should know and understand what the ‘rules of appropriate use’ are and what sanctions result from misuse.
- Should know to never make contact with any student via personal devices or social media networks.
- Should know to never “friend” a student or ex-student on their personal social media networks. (Unless that person has attained the age of 18).
- Should know that all communication with a student should be face to face or via an approved school e mail system and never on a personal device or through a personal social media platform.

All adults in our school community will ensure that in private use:

- No reference should be made in social media to pupils, parents / carers or school staff.
- Personal phone/ mobile phone numbers and email addresses (i.e. non-school or LGfL London Grid for Learning addresses) are not divulged to pupils
- They do not engage or interact with pupils on social media sites.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

I will maintain a professional level of conduct in my personal use of technology, both within and outside school.

I will not engage in any online activity that may compromise my professional responsibilities

I have read and understand these rules and agree to them.

Name: ***Staff***

Signed: ***Date:***

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 acceptable use agreement 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: online safety incident report log

Online safety incident report log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident