**St Peter at Gowts Church of England Primary School**

| | |
|---|---|
| **Policy** | **eSafety** |
| **Date adopted** | **September 2015** |
| **Date reviewed** | **December 2018** |

**Policy Statement**

For clarity, the eSafety policy uses the following terms unless otherwise stated:

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

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

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

**Wider school community** – students, all staff, governing body, parents, friends and family.

Safeguarding is a serious matter; at St Peter at Gowts CE Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as eSafety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an eSafety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the St Peter at Gowts CE Primary School website; upon review all members of staff will sign as read and understood both the eSafety policy, Staff ICT Acceptable Use policy and Staff use of school and personal device policy December 2018. A copy of this policy and the Students Acceptable Use Policy will be shared will all parents currently at and new to the school.

All these mentioned policies are found as the appendix in this policy.

**Policy Governance (Roles & Responsibilities)**

**Governing Body**

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

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

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

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

**Headteacher**

Reporting to the governing body, the Headteacher has overall responsibility for eSafety within our school. She will act as the eSafety Officer, as indicated below.

The Headteacher will ensure that:

- eSafety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated eSafety Officer has had appropriate CPD in order to undertake the day to day duties.
- All eSafety incidents are dealt with promptly and appropriately.
- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the governing body.
- Advise the governing body on all eSafety matters.
- Engage with parents and the school community on eSafety matters at school and/or at home.
- Liaise with the local authority, ICT technical support and other agencies as required.
- Retain responsibility for the eSafety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical eSafety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make herself aware of any reporting function with technical eSafety measures, i.e. Internet filtering reporting function; liaise with the responsible governor to decide on what reports may be appropriate for viewing.

**All Staff**

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any eSafety incident is reported to the eSafety Officer (and an eSafety Incident report is made.

**All Students**

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

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

**Parents and Carers**

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

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded.

**Technology**

St Peter at Gowts CE Primary School uses a range of devices including latops, MacBooks and iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

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

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

**Encryption** – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner'sOffice. *(Note: Encryption does <u>not</u> mean password protected.)*

**Passwords** – all staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change on a regular basis or if there has been a compromise. The ICT Coordinator and ICT Support will be responsible for ensuring that passwords are changed.

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

**Safe Use**

**Internet** – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this eSafety and the staff Acceptable Use Policy (appendix); students upon signing and returning their acceptance of the Acceptable Use Policy (appendix).

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

**Photos and videos** – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip on entry to the school.

**Social Networking** – there are many social networking services available; St Peter at Gowts CE Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within St Peter at Gowts CE Primary School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the eSafety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Twitter – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

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

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

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

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

**Training and Curriculum** - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, St Peter at Gowts CE Primary School will have an annual programme of training which is suitable to the audience.

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

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

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

# Acceptable Use Policy – Staff

All adults working with ICT equipment within St Peter at Gowts Church of England Primary School must ensure and agree to abide by the Staff ICT Acceptable Use Policy.

**For personal use:**

- Do not give anyone access to your login name or password.
- Do not introduce any removable media into the system without first having them checked for viruses.
- Do not open other people's files without express permission.
- Do not corrupt, interfere with or destroy any other user's information.
- Do not release personal details including phone numbers, fax numbers or personal e-mail addresses of any colleague or pupil over the Internet.
- Do not reproduce copyright materials without first getting permission from the owner. Many people will make their work freely available for education on request. Acknowledge sources on all resources used.
- Do not attempt to visit sites which might be considered inappropriate. All sites visited leave evidence on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
- Use of school Internet access for business, profit, advertising or political purposes is strictly forbidden.
- Users should log out when their session has finished.
- Any personal files or documents (including photos) should not be stored on schools ICT equipment.

**Personal E-mail**

- Observe *netiquette* on all occasions. E-mail should not be considered a private medium of communication.
- Do not include offensive or abusive language in your messages or any language which could be considered defamatory, obscene, menacing or illegal.
- Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority.
- Make sure nothing in the messages could be interpreted as libelous.
- Do not send any message which is likely to cause annoyance, inconvenience or needless anxiety.
- Do not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes.

**When using the Internet**

- Ensure that your web activities conform to the norms of moral decency.
- Watch for accidental access to inappropriate materials and report the offending site to the designated person that deals with filtering.
- Check before publishing work; make sure that you have Copyright holder's permission.
- Ensure children cannot be identified from photographs.
- Report any breaches of the Internet policy to the designated person.

# Staff use of school and personal devices

## Storing of data

If it is necessary for you to take work home, or off site, you may only do so on a school MacBook or laptop (as these are encrypted). Any hard drives used to store photos or planning from previous years must be kept onsite. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

## Use of school devices

Usage of all devices by staff should be in line with the Staff Acceptable Use Policy. All teaching staff are given a MacBook and an iPad to use in school and at home for school purposes. Some classroom-based staff may be given access to their own individual iPad to use in school and at home for school purposes. In addition to this, access may be granted to classroom-based staff to use a MacBook in school and home for school purposes. This will need to be agreed by the Head Teacher and ICT lead. All devices remain the property of the school and must be returned when requested (ie. if on long term sick or maternity leave) or when leaving the school**.** Staff will not load or open inappropriate websites, games or materials of any kind onto devices**.** Use of home Internet services are permitted in line with the Staff Acceptable Use Policy. Staff are able to load free apps onto devices for educational purposes. If there is a paid app, staff can make a request to the ICT lead who will arrange for the app to be loaded onto all school equipment, if deemed appropriate. Social networking sites that are not used in school are prohibited to be used on any device, including downloadable Apps. Staff members will be expected to pay in full for any costs of any damage or loss to their device should it be broken or lost outside of school or through negligence.

## Use of Personal ICT equipment

Staff in school are allowed to access Twitter on their school computers, iPads and iPods. This will include the taking of photos and posting of Tweets. There may be occasions when staff will use their mobile phone to take photos and upload them to Twitter and post Tweets. The school deems this as appropriate in line with the staff acceptable use policies. Any staff member using their mobile phone in school is responsible for ensuring the photos take are deleted after being uploaded to Twitter. Photos and videos will be deleted by the end of the day they were taken. All staff have access to an iPad and therefore have no need use personal iPads in the classroom.

## Digital cameras

Any photographs or videos taken on digital cameras are to be uploaded at the earliest possible convenience and deleted from the camera. Digital cameras should remain on site, unless they are taken on a school trip. On a school trip, the class teacher is responsible for the digital camera and needs to store it in a safe place.

## Using the school Internet

Staff are permitted to use the school Internet on personal devices in accordance with the Staff Acceptable Use Policy.

**Acceptable Use Policy – Students**

**Note: All Internet and email activity is subject to monitoring**

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

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

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

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

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

**I will not** – share my password with anybody. If I forget my password I will let my teacher know.

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

**I will not** – share personal information online with anyone.

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

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

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

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

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

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

**Signed (Parent) :**

**Signed (Student) :**

**Date :**