Syresham St. James CE Primary School

e-safety Policy

Policy Statement

For clarity, the e-safety 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.

Syresham St James Primary School seeks to create an environment that reflects our Christian ethos, providing safe, happy and challenging working conditions for all members of the school. This environment is exemplified by our school values to promote respect, generosity, courage, love, fairness and forgiveness.

Safeguarding is a serious matter; at Syresham School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety 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 School website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy is available on the website and the Students Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Headteacher: Kate Clough Signed:

Chair of Governors: Clare Powell Signed:

Review Date: 15th January 2016 Next Review:

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 e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety 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 e-safety at the school who will:

    - Keep up to date with emerging risks and threats through technology use.
    - Ensure that the Headteacher, as e-Safety Officer, has had appropriate CPD in order to undertake the day-to-day duties of the role.

    Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

The e-safety Governor is Mr Jonathan Stone.

Headteacher

Reporting to the governing body, the Headteacher, who is the e-Safety Officer, has overall responsibility for e-safety within our school.

The Headteacher will ensure that:

- e -Safety 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.
- All e-safety incidents are dealt with promptly and appropriately.

As the e-Safety Officer, the Headteacher will:

- 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 e-Safety Governor.
- Advise the governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety 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 him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the e-Safety Governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
  - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
  - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
  - Any e-safety technical solutions such as Internet filtering are operating correctly.
  - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Headteacher/e-Safety officer.
  - Passwords are applied correctly to all users regardless of age.

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 e-safety incident is reported to the Headteacher/e-Safety Officer and recorded in the e-Safety Incident report book. If you are unsure the matter is to be raised with the Headteacher/e-Safety Officer to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

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.

e-Safety 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 and school surveys the school will keep parents up to date with new and emerging e-safety 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. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

e-Safety Governor

Is responsible for e-Safety at school;

- to advise on changes to the e-safety policy.
- to establish the effectiveness (or not) of e-safety training and awareness in the school.
- to recommend further initiatives for e-safety training and awareness at the school.

The e-Safety Governor will meet with Headteacher/e-Safety Officer on a termly basis.

Technology

Syresham Primary School uses a range of devices including PC's, laptops, Apple Macs. 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 exa-networks.co.uk 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 Headteacher/e-Safety Officer is responsible for ensuring that the filtering is appropriate.

Email Filtering – we use exa-networks.co.uk 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.

Data Protection – Staff must take reasonable precautions with all school devices that hold personal data. 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's Office.

Passwords – all staff and students will be unable to access any device except guest accounts on class and hall laptops without a unique username and password. Staff and student passwords will change annually or if there has been a compromise, whichever is sooner. IT 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 automatically. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

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 e-Safety Policy and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the emails should be kept professional.
Students are permitted to use the school email system, and as such will be given their own email address.

Photos and videos and phones –All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

- All staff must ensure that their mobile phones, personal cameras and recording devices are stored securely during working hours on school premises or when on outings. (This includes visitors, volunteers and students).
- Photos should be put on the school system as soon as possible and not sent to or kept on personal devices. Personal devices should only be used with permission of the headteacher.
- During school outings nominated staff will have access to a school mobile which can be used for emergency or contact purposes.

- All telephone contact with parents or carers must be made on the school phone and a note kept.
- Parents or carers are permitted to take photographs of their own children during a school production or event. The school protocol requires that photos of other people's children are not published on social networking sites such as Facebook.
- Staff and parents are advised against the misuse of network sites such as Facebook and Twitter to share confidential or potentially negative or abusive comments or information regarding the school, a member of staff, parent or child. See e-safety policy.

Social Networking – there are many social networking services available; however Syresham only uses the School Website as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The Website has been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer/Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

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

- Permission slips (via the school Policy for the use of images) 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 license 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 e-safety incident is to be brought to the immediate attention of the Headteacher/e-Safety Officer. The Headteacher/e-Safety 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, Syresham will have an annual programme of training which is suitable to the audience.

e-Safety 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 Headteacher/e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the 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 Headteacher for further CPD.

The e-Safety Training Programme can be found in the Headteacher's office.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the Headteacher/e-Safety Officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff are advised not to become "friends" with parents or pupils on personal social networks

Use of Email – All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, take reasonable precautions to ensure that your device is kept secure.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the Headteacher/e-Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the Headteacher/Bursar as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

NAME :

SIGNATURE : **DATE :**

Acceptable Use Policy – KS2 Students

Our Charter of Good Online Behaviour

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. 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 will – be open about my online activities.

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.

I understand – what to do if I see something inappropriate on the computer or iPad

Signed (Parent) :

Signed (Student) :

Date :

Acceptable Use Policy – EYFS/KS1 Students

Our Charter of Good Online Behaviour

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 – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – use other people's usernames or passwords. If I forget my password I will let my teacher know.

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 will – be open about my online activities.

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

I understand – what to do if I see something that concerns or upsets me on the computer or iPad

Signed (Parent) :

Signed (Student) :

Date :