Sessay CE Primary School

E – SAFETY POLICY
2016 – 2019

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At **Sessay C of E School,** we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.
Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.
Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

Monitoring
All internet activity is logged by the school's internet provider. These logs may be monitored by authorised NYCC staff.

Breaches
A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.
Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, where appropriate, the NYCC Disciplinary Procedure or Probationary Service Policy.

Policy breaches may also lead to criminal or civil proceedings.

The ICO's new powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

- The data protection powers of the Information Commissioner's Office are to: Conduct assessments to check organisations are complying with the Act;Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher or Senior Teacher. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the headteacher.

Computer viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick, must be checked for any viruses using school provided anti-virus software before being used
- Never interfere with any anti-virus software installed on school ICT equipment that you use
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact NYCC school's ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

The use of email

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette. In order to achieve ICT age related expectations, pupils must have experienced sending and receiving e-mails:

- The school will provide all staff their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
    - Delete all e-mails of short-term value
      Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
      Staff must inform headteacher if they receive an offensive e-mail
      However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply
      Pupils are introduced to e-mail as part of the ICT Curriculum.
      All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
      Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail

Equal opportunities

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules.

However, staff are aware that some pupils may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

E-safety Role sand responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in this school is Katie Tyrka- Senior Teacher **i**t is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as NYCC LA, CEOP (Child Exploitation and Online Protection) and Childnet.

All staff and governors are updated by the Head and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. Pam Laycock, Safeguarding Governor has an overview. This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHCE

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

- The school has a framework for teaching internet skills in ICT/ PSHE lessons.

- The school provides opportunities within a range of curriculum areas to teach about e-Safety

- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-Safety curriculum

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities

- Pupils are aware of the impact of Cyber-bullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

E-Safety Skills Development for Staff

Our staffs receive regular information and training on e-Safety and how they can promote the 'Stay Safe' online messages, this is identified through the CPD master plan.

- New staff receive information on the school's acceptable use policy as part of their induction

- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowcharts)

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Managing the School e-Safety Messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used

- The e-Safety policy will be introduced to the pupils at the start of each school year

- E-Safety posters will be prominently displayed (these are available on the server)

- The key e-Safety advice will be promoted widely through school displays, newsletters, class activities.

SESSAY C of E PRIMARY SCHOOL

Rules for Responsible Internet Use

The school is very pleased to be able to offer access to the Internet in our computer suite, from any of the computers. However it is important that everyone understands that the Internet needs to be used carefully. These rules will help to achieve that.

Pupils: -

- I will only access the Internet or e-mail account when my teacher has given me permission to do so.
- I will only visit web sites that my teacher has approved for use.
- I will only send e-mails to people that my teacher has approved.
- I will not give my home address or telephone number, or that of anyone else unless I have been given permission to do so by my parents and my teacher.
- I will immediately report any unpleasant message which I have been sent.
- I understand that the school can check to see which Internet sites I have visited.
- I understand that I am responsible if I access unpleasant material on the Internet because I have not followed my teacher's instructions.

The School: -

- We will ensure that the children are only directed to sites with appropriate material.
- We will establish the appropriateness of sites prior to lessons.
- We will provide opportunities for children to appreciate the huge possibilities which the Internet offers for learning.

.....

I have read and understood the above contract and agree to abide by the rule set out.

Signed ..... Class .....

I give permission for my child to have supervised access to the Internet at school

Signed .....