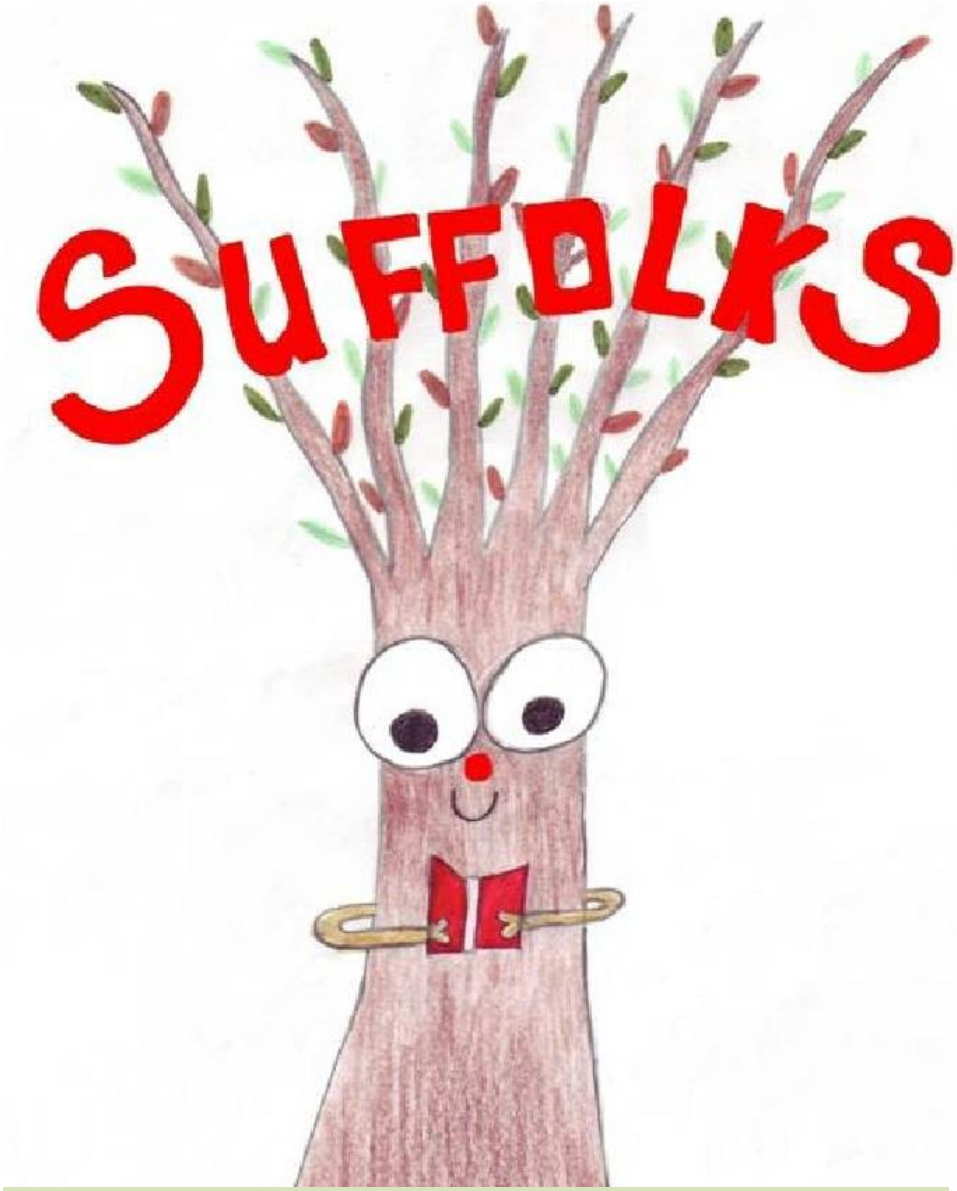
Summer 2016

‘FROM GREAT TO AMAZING’

Suffolks Primary School E Safety



SUCCESS, UNIQUENESS, ENVIRONMENT, COMMUNITY

Implemented : September 2016

To be reviewed : April 2017

Review frequency Initially Annually

Consultation process

- Staff (September 2016)
- Pupils (January 2016)
- Governors (October 2016)

Signed _____ (HT)
Signed _____ (CoG)

e-Safety Policy

The Acceptable Use of the Internet and related Technologies
Our e-Safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed ICT is now seen as a functional, essential life skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet can benefit the professional work of staff and enhances the school's management information and business administration systems.

Whole school approach to the safe use of ICT
Creating a safe ICT learning environment includes three main elements at this school:
• An effective range of technological tools;
• Policies and procedures, with clear roles and responsibilities;
• A comprehensive e-Safety education programme for pupils, staff and parents

The risks
The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people. Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. At Suffolks we are committed to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk.

We are fully aware of the role that the internet can play in grooming children in terms of sexual exploitation and in developing and sharing extremist views. All staff have yearly training and induction on our child protection and safeguarding procedures which includes process for raising concerns regarding radicalisation and exploitation.

The technologies
New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:
• The Internet
• e-mail
• Instant messaging often using simple web cams
• Blogs (an on-line interactive diary)
• Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
• Social networking sites
• Video broadcasting sites
• Chat Rooms
• Gaming Sites
• Music download sites
• Mobile phones with camera and video functionality
• Smart phones with e-mail, web functionality and cut down ‘Office’ applications.
Although the majority of these are not used in school, staff and children should be aware of the risks involved when using these technologies.

Roles and Responsibilities
e-Safety is recognised as an essential aspect of strategic leadership in this school and the headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored. Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-

Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP). The school's e-Safety coordinator ensures the Headteacher is updated as necessary.
All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. All staff should be familiar with the schools' Policy including:
• Safe use of e-mail;
• Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
• Safe use of school network, equipment and data;
• Safe use of digital images and digital technologies, such as digital cameras;
• publication of pupil information/photographs and use of website;
• eBullying / Cyberbullying procedures;
• their role in providing e-Safety education for pupils

We are committed to ensuring that all children are safe from radicalisation and extremism online. The e-Safety coordinator will ensure that staff and children are schooled and up to date with current developments through CEOP training. Any concerns will be reported through the use of pink sheets and refereed to the designated child protection officer.

System Safety Measures
The school maintains broadband connectivity through the HGfL and so connects to the National Education Network. Additionally, the school has up-to-date antivirus, anti-spyware and anti-spamware software and approved firewall solutions installed on their network. To make sure rogue applications are not downloaded and hackers cannot gain access to the school's equipment or into users' files through Internet use, staff and pupils are not able to download executable files and software. Unfortunately, there is the potential for inappropriate material to get through any filtering system. Access to inappropriate sites can be blocked.
This school:
• Works in partnership with the HGfL to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect students;
• Ensures network health through appropriate anti-virus software and network set-up so staff and pupils cannot download executable files such as .exe /.com / .vbs etc.;
• Ensures their network is 'healthy' by having HGfL health checks annually on the network;
• Utilises caching as part of the network set-up;
• Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies;
• Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
• Has network auditing software installed;
• Never sends personal data over the Internet unless it is encrypted or otherwise secured.

Surfing the Web
Aimless surfing should never be allowed. Pupils should be taught to use the Internet in response to an articulated need e.g. a question arising from work in class. Search engines can be difficult to use effectively. The teacher will need to choose a topic with care, select the search engine and then discuss with pupils sensible search words, which should be tested beforehand. Although Suffolks internet is provided by LGFL who have strict filtering systems there are also child-friendly search engines available for added security.

Education Programme:
Pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering and monitoring. This school:
• Fosters a 'No Blame' environment that encourages pupils to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable;
• Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or ICT co-ordinator;
• Has a clear, progressive e-safety education programme throughout all Key Stages, built on LA / LGfL / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

o to STOP and THINK before they CLICK
o to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
o to discriminate between fact, fiction and opinion; o to develop a range of strategies to validate and verify information before accepting its accuracy;
o to skim and scan information;
o to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
o to know some search engines / web sites that are more likely to bring effective results;
o to know how to narrow down or refine a search;
o [for older pupils] to understand how search engines work;
o to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
o to understand 'Netiquette' behaviour when using an online environment such as a 'chat' / discussion forum, i.e. no bad language, propositions, or other inappropriate behaviour;
o to not download any files – such as music files – without permission;
o to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos;
o to have strategies for dealing with receipt of inappropriate materials.
• Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
• Makes training available annually to staff on the e-safety education program;
• Runs a rolling programme of advice, guidance and training for parents, including:
o Information in safety leaflets; in school newsletters; on the school web site;
o demonstrations, practical sessions held at school;
o suggestions for safe Internet use at home;
o provision of information about national support sites for parents.

How will e-mail be managed?
E-mail is now an essential means of communication for staff in our school and increasingly for pupils and homes. Directed e-mail use in schools can bring significant educational benefits through increased ease of communication between students and staff, or within local and international school projects. Schools in London have an appropriate educational, filtered Internet-based e-mail system through the London Grid for Learning (LGfL).

Technology:
Incoming and outgoing e-mail can be restricted to approved addresses and filtered for unsuitable content and viruses. This is the first line of defence. By default any pupil accounts that are created are automatically assigned as 'safe mail'. This means that they can only exchange e-mails with pupils and teachers from the same school. If a teacher wants to open up a class or a year group for a certain amount of time or permanently, they can do this by removing the safe mail restriction. This means that they would have a typical e-mail account that is able to send or receive e-mails with anyone. All e-mails in the LGfL system go through a filtering process for inappropriate language regardless of whether they are in safe mail or not. Where the school receives nuisance or bullying e-mails and the e-mail address of the sender is not obvious, it is possible to track the address using 'e-mail' tracking software. Talk to your LEA where necessary.

Procedures
In the school context, e-mail should not be considered private and most schools, and indeed Councils and businesses, reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation. Whole-class or project LGfL e-mail addresses can be used in primary schools, to communicate outside the school community.
• Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses.
• If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the police.
• Accounts are managed effectively, with up to date account details of users.

• Pupils can only use the LGfL / school domain e-mail accounts on the school system.
• Staff can only use the LGfL / school domain e-mail accounts on the school system.
• Pupils are introduced to, and use e-mail as part of the ICT scheme of work.
• Pupils are first introduced to principles of e-mail through closed 'simulation' software.
• Pupils are taught about the safety and 'netiquette' of using e-mail i.e.
    o not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer;
    o that an e-mail is a form of publishing where the message should be clear, short and concise;
    o that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
    o they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
    o to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    o the sending of attachments should be limited;
    o embedding adverts is not allowed;
    o that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    o not to respond to malicious or threatening messages,
    o not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    o not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    o that forwarding 'chain' e-mail letters is not permitted;
• Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.
• Staff sign the appropriate LA / school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Using Digital Images and Video Safely

Developing safe school web sites
The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety. A senior member of staff needs to oversee / authorise the website's content and check suitability. It should be clear who has authority to upload content into sections of the website. Having a website that is easy to maintain and update is helpful and many schools use one of the LGfL templates as a basis for this. This portal functionality is included within the broadband package.

Use of still and moving images
Most importantly, take care when using photographs or video footage of pupils on the school website. Consider using group photographs rather than photos of individual children. Do not use the first name and last name of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the school. An easy rule to remember is:
G **If the pupil is named, avoid using their photograph / video footage.**
G **If the photograph /video is used, avoid naming the pupil.**
If showcasing examples of pupils work consider using only their first names, rather than their full names. Only use images of pupils in suitable dress to reduce the risk of inappropriate use. In many cases, it is unlikely that the Data Protection Act will apply to the taking of images e.g. photographs taken for personal use, such as those taken by parents or grandparents at a school play or sports day. However, photographs taken for official school use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, pupils and students should be advised why they are being taken. Parental permission should be obtained before publishing any photographs, video footage etc of pupils on the school website or in a DVD. This ensures that parents are aware of the way the image of their child is representing the school. A Parental Permission Form is an appropriate way of achieving this.

Procedures:

Use excerpts of pupils' work such as from written work, scanned images of artwork or photographs of items designed and made in technology lessons. This allows pupils to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of pupils. Links to any external websites should be thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience. Remember that the content of websites can change substantially, even in a short space of time. Check all links regularly, not only to ensure that they are still active, but that the content remains suitable too. Text written by pupils should always be reviewed before publishing it on the school website. Make sure that the work doesn't include the full name of the pupil, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them. Although it may seem obvious, check that pupils' work doesn't contain any statements that could be deemed defamatory. Ensure also that the school is not infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought. If the school's website contains any guestbook, noticeboard or blog, they need to be monitored to ensure they do not contain personal details of staff or pupils. If the school website is using a webcam – then this must be checked and monitored to ensure misuse does not occur accidentally or otherwise. If showcasing school-made digital video work, take care to ensure that pupils are not referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film. Digital images - photographs and video clips - can now readily be taken using mobile phones. Extreme abuse is the so called 'happy slapping' incidents sent to others or posted onto a website, e.g. a recent case of a posting on YouTube. It is therefore important to ensure that the risk of inappropriate use is minimised. Staff should be advised not to use their personal phone or camera without permission e.g. for a school field trip. If personal equipment is being used it should be registered with the school and a clear undertaking that photographs will be transferred to the school network and will not be stored at home or on memory sticks and used for any other purpose than school approved business.

Education:
Ensure staff and pupils know who to report any inappropriate use of images to and understand the importance of safe practice. Staff and pupils also need to understand how to consider an external 'audience' when publishing or presenting work.
In this school:
• The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
• Uploading of information is restricted to Headteacher and LGFL technician.
• The school web site complies with the school's guidelines for publications;
• Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
• The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
• Photographs published on the web do not have full names attached;
• We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
• Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted when children leave the school – unless an item is specifically kept for a key school publication;
• We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
• We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
• Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
• Pupils are only able to publish to their own 'safe' web-portal on the LGfL in school;
• Pupils are taught about how images can be abused in their eSafety education programme.

How will infringements be handled?
Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

Students

Category A infringements:
• Use of non-educational sites during lessons
• Unauthorised use of email
• Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
• Use of unauthorised instant messaging / social networking sites

Sanctions: referred to class teacher.

Category B infringements
• Continued use of non-educational sites during lessons after being warned
• Continued unauthorised use of email after being warned
• Continued unauthorised use of mobile phone (or other new technologies) after being warned
• Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups
• Use of File sharing software e.g. music sharing software
• Accidentally corrupting or destroying others' data without notifying a member of staff of it
• Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Sanctions: referred to Class teacher, e-safety Coordinator / removal of Internet access rights for a period / contact with parent.

Category C infringements
• Deliberately corrupting or destroying someone's data, violating privacy of others
• Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
• Deliberately trying to access offensive or pornographic material
• Any purchasing or ordering of items over the Internet
• Transmission of commercial or advertising material

Sanctions: as category B and referred to deputy head.

Other safeguarding actions
If inappropriate web material is accessed:
1. Ensure appropriate technical support filters the site
2. Inform LgFL

Category D infringements
• Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
• Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
• Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
• Bringing the school name into disrepute

Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / removal of equipment / refer to Community Police Officer / LA e-safety officer

Other safeguarding actions:
1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

Staff
Category A infringements (Misconduct)
• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
• Misuse of first level data security, e.g. wrongful use of passwords
• Breaching copyright or license e.g. installing unlicensed software on network

Sanction - referred to line manager / Headteacher. Warning given.

Category B infringements (Gross Misconduct)
• Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
• Any deliberate attempt to breach data protection or computer security rules;
• Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
• Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
• Bringing the school name into disrepute.

Sanction - referred to line manager / Headteacher.

Principles and criteria for good practice

The key is to ensure that children have access to ICT which offers them opportunities to develop general skills and also extends their specific knowledge of that technology. Given the range of computer hardware and software now available on the educational and toy market it has become increasingly difficult to make informed choices between them. DATEC's publication of guidance material for parents and practitioners is therefore calculated to provide for a pressing community need. It is based on research with practitioners and researchers in the field.

A growing consensus has emerged regarding the most appropriate forms that ICT education should take in early childhood. Seven general principles have been identified for determining the effectiveness of ICT applications – or uses of ICT – in the early years, to help practitioners provide the best possible experiences. They are:
1 ensure an educational purpose
2 encourage collaboration
3 integrate with other aspects of curriculum
4 ensure the child is in control
5 choose applications that are transparent
6 avoid applications containing violence or stereotyping
7 be aware of health and safety issues.

For more details please see separate report *Developmentally Appropriate Technology in Early Childhood (DATEC) Final Report – also reproduced in Siraj-Blatchford, I. and Siraj-Blatchford, J. (2000) More than Computers: Information and Communications Technology in the Early Years, London, Early Education (The British Association for Early Childhood Education)*