# Willowbrook Primary School

## eSafety and Data Security



Responsible person: Lisa McAdams
Adopted: May 2016
Review: May 2019
Willowbrook Primary

**CONTENTS**

Acknowledgement

Senior Information Risk Officer - The SIRO in this school is the Headteacher.

Information Asset Owner – The IAO is the School Business Manager.

e-Safety Officer – The e-Safety officer is the Inclusion Manager

## Introduction

ICT in the 21st Century is 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. ICT covers a range of resources including web-based and mobile learning.

It is important to recognise the fast paced evolution of technology within our society as a whole. 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.

At Willowbrook Primary School, we understand the responsibility to educate our pupils on eSafety 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 our 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, personal digital assistants (PDAs), tablets, 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, camera phones, PDAs and portable media players, etc).

Monitoring

Authorised Computing staff may inspect any computing equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge. Any Computing authorised staff member will be happy to comply with this request.

Computing authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School Computing; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

Computing authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by Computing authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School Computing may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised Essex County Council (ECC) 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 Computing 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 Essex County Council Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

## 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 school's Senior Information Risk Owner (SIRO) or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the SIRO.

See flowcharts on page 14 for dealing with both illegal and non-illegal incidents.

## Acceptable Use Agreement: Pupils

**Willowbrook Primary School Computing Code of Conduct (Acceptable Use Agreement / eSafety Rules)**

Using the computers:
I will only use ICT in school for school purposes.
I will not tell other people my passwords.
I will only open/delete my own files.
I will only access the computer system with the login and password I have been given.
I will not access other people's files or bring in USB drives or CDs from outside school.

Using the internet:
I will ask permission from a teacher before using the internet or sending an email.
I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself.
I understand that the school may check my computer files and may monitor the internet sites I visit.
I will not complete and send forms without permission from my teacher.
I will not give out personal information, including but not limited to my full name, my home address or telephone number.
I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.

Using e-mail:
I will immediately report any unpleasant messages sent to me because this would help protect other pupils and myself.
I understand that e-mail messages I receive or send may be read by others.
The messages I send will be polite and responsible.
I will only e-mail people I know, or my teacher has approved.
I will only use my class e-mail address or my own school e-mail address when e-mailing.
I will only open e-mail attachments from people I know, or who my teacher has approved.
I will not give my personal details out, including my full name, my home address or telephone number.
I will not use e-mail to arrange to meet someone outside school hours.

I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my eSafety.

Name …… Date …….

Parents are asked to read and discuss these eSafety rules with their child in order to ensure that all children are safe and responsible when using any ICT.

**Acceptable Use Agreement: Staff, Governors and Visitors**

**Staff, Governor and Visitor**
**Acceptable Use Agreement / Code of Conduct**

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher, or the eSafety Coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of eSafety Coordinator or IT Technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

This Acceptable Use Agreement is a summary of the eSafety Policy which is available in full via the school website.

**User Signature**

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature …… Date ……..

Full Name ……..(printed)

Job title……

## Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. flash stick, CD) must be checked for any viruses using school provided anti-virus software before using them
- Never interfere with any anti-virus software installed on school equipment that you use
- If you suspect there may be a virus/malware on any school Computing equipment, stop using the equipment and contact your IT Technician or eSafety Coordinator immediately. They will advise you what actions to take and be responsible for advising others that need to know

## Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

The safe use of new technologies - Ofsted
http://webarchive.nationalarchives.gov.uk/20120408131156/http:/www.ofsted.gov.uk/resources/safe-use-of-new-technologies

Inspecting e-safety – Ofsted
http://www.kelsi.org.uk/__data/assets/pdf_file/0008/28871/Inspecting-e-safety-Ofsted.pdf

Teachers' and Governors' Guidance
http://webarchive.nationalarchives.gov.uk/20130401151715/http://www.education.gov.uk/publications/eOrderingDownload/Working%20Smarter%20Booklet.pdf

Internet filtering for Essex Schools
https://schools-secure.essex.gov.uk/admin/Broadband/School%20Services/Pages/InternetFilteringSecurity.aspx

e-Safety Audit Tool - Information for Governors, Management and Teachers
http://www.nen.gov.uk/e-safeguarding-tool/

## Security

- The School gives relevant staff access to its Management Information System, with a unique ID

and password

- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for Computing Acceptable Use
- Leadership have identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO)
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always keep portable and mobile ICT equipment or removable media under their control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed

**Senior Information Risk Owner (SIRO)**

The SIRO is a senior member of staff who is familiar with information risks and the school's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

- they appoint the Information Asset Owner(s) (IAOs)
- they act as an advocate for information risk management

The Office of Public Sector Information has produced 'Managing Information Risk' [https://www.gov.uk/guidance/managing-information-risk] to support SIROs in their role.

The SIRO in this school is the Headteacher.

**Information Asset Owner (IAO)**

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff, such as assessment records, medical information and special educational needs data. The

Information Asset Owner in this school is the School Business Manager.

The role of an IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, pupil or staff etc including UPN, teacher DCSF number etc)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

**Disposal of Redundant ICT Equipment Policy**

- All redundant ICT equipment will be disposed of through an authorised agency.
- All redundant equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.
- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- The school's disposal record will include:
    - Date item disposed of
    - Authorisation for disposal, including:
        - verification of software licensing
        - any personal data likely to be held on the storage media? *
    - How it was disposed of e.g. waste, gift, sale

- Name of person and / or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

## e-Mail

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; 'netiquette'.

### Managing e-Mail

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all pupil mail is filtered and logged; if necessary e-mail histories can be traced. The school email account is the preferred account that is used for school business
- Under no circumstances should staff contact pupils or parents using personal e-mail addresses
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- 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; they must not arrange to meet anyone without specific permission, and should virus check all attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform the eSafety co-ordinator or IT Technician if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the Computing Scheme of Work
- 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

### Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section e-mailing Personal, Sensitive, Confidential or Classified Information
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

- School e-mail is not to be used for personal advertising

**Receiving e-Mails**

- Check your e-mail regularly
- Never open attachments from an untrusted source, consult your IT support first.

**e-mailing Personal, Sensitive, Confidential or Classified Information**

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided wherever possible
- Where your conclusion is that e-mail must be used to transmit such data:
  - Obtain express consent from your manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
    - Verify the details, including accurate e-mail address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
  - Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s) – preferably by telephone
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies. Such arrangements are currently in place with:

- Essex Police
- District and Borough Councils within Essex County Council
- Essex NHS Trusts

When sending e-mails with information about a pupil, the name of the individual is not to be included in the subject line and the document containing the information should be encrypted. This provides additional security.

## Equal Opportunities

**Pupils with Additional Needs**

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 school's eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

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

## eSafety - Roles and Responsibilities

As eSafety 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 eSafety Co-ordinator in this school is the Inclusion Co-ordinator, who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety Co-ordinator to keep abreast of current issues and guidance through organisations such ECC, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/eSafety Co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

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, safeguarding, health and safety, home–school agreements, behaviour (including anti-bullying) and PSHE.

## eSafety in the Curriculum

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

- The school has a framework for teaching internet skills in Computing / PSHE lessons
- The school provides opportunities within a range of curriculum areas to learn about eSafety
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the eSafety 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 and respecting other people's information, images, etc through discussion, modeling and activities

- Pupils are aware of the impact of Cyberbullying 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 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 Computing curriculum

**eSafety Skills Development for Staff**

- Our staff receive regular information and training on eSafety issues in the form of PDM

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

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

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

**Managing the School eSafety Messages**

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

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

- eSafety posters are prominently displayed

**Incident Reporting, eSafety Incident Log & Infringements**

**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 school's SIRO or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Senior Information Risk Owner.

## eSafety Incident Log

Details of all eSafety incidents will be recorded by the eSafety Co-ordinator. Some incidents may need to be recorded in other places, if they relate to a bullying or racist incident. These will be recorded in the Headteacher's office.

## Misuse and Infringements

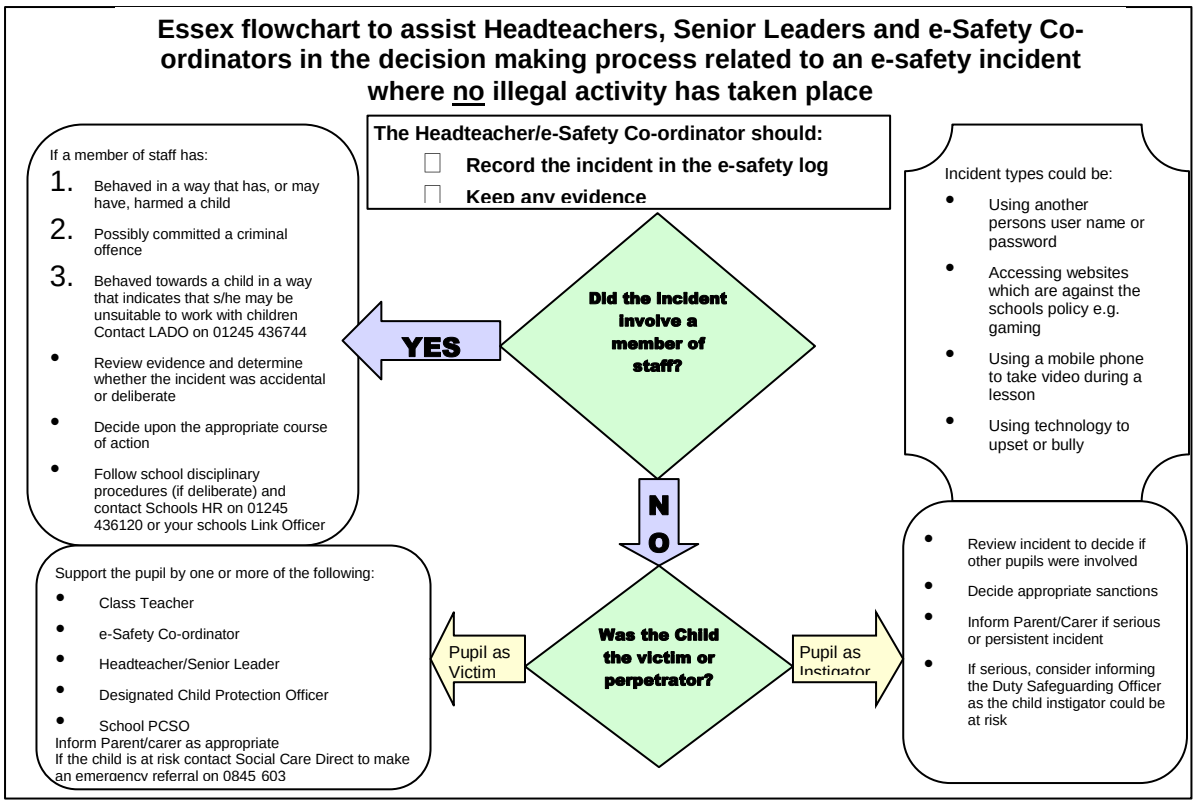
### Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety Co-ordinator or Headteacher. Incidents should be logged and the **Essex Flowcharts for Managing an eSafety Incident** should be followed.

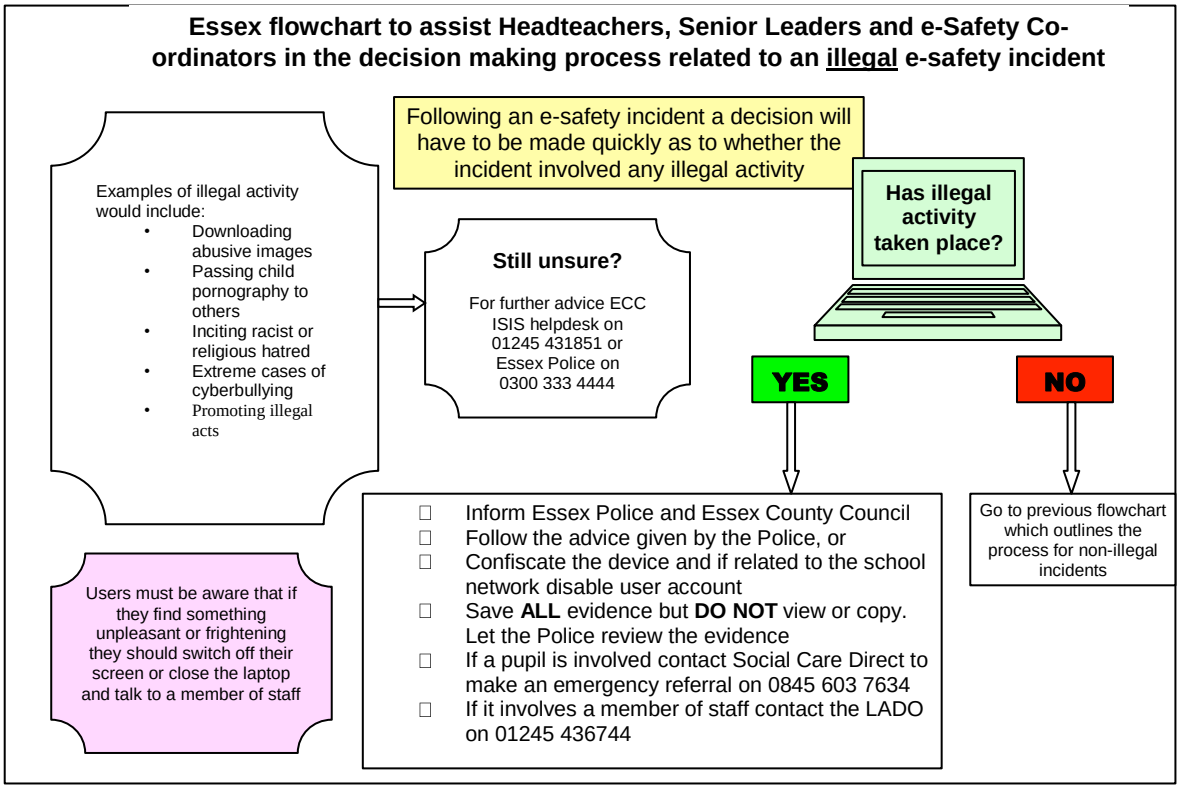
### Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety Co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety Co-ordinator. Depending on the seriousness of the offence there may be investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

## Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an e-safety incident where no illegal activity has taken place




## Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an illegal e-safety incident






Responsible person: Lisa McAdams
Adopted: May 2016
Review: May 2019
Willowbrook Primary

## Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

## Managing the Internet

- In school, children have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with pupils, or checked by the teacher first and google/bing filters used as well as county filters
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher - it is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times; it is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources
- Every effort is made to ensure children are safe when accessing the Internet; this includes training staff on how to protect children from any form of radicalisation, extremism or cyber bullying (see the school website http://www.willowbrook.essex.sch.uk/school-policies/ for policies on Keeping Children Safe in Education 2015 and Child Protection Policy 2015)

## Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog
- On-line gambling is not allowed

It is at the Headteacher's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

**Infrastucture**

- Essex County Council has a monitoring solution where web-based activity is monitored and recorded
- School internet access is controlled through the LA's web filtering service. For further information relating to filtering please email essexcc-servicedesk.sen.uk@siemens-enterprise.com
- Willowbrook is aware of its responsibility when monitoring staff communication under current legislation and takes into account Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the eSafety Co-ordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines
- If there are any issues related to viruses or anti-virus software, the network manager should be informed

**Managing Other Web 2 Technologies**

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking sites to pupils within school
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online

- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)

- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online

- Our pupils are asked to report any incidents of bullying or strangers who have attempted to make contact to the school

## Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to Computing and associated risks.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- Parents/ carers are required to make a decision as to whether they consent to images and videos of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items
    - Learning platform training

## Passwords and Password Security

**Passwords**

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised Computing support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Passwords must contain a minimum of six characters, mixed letters and numbers and be difficult to guess
- User ID and passwords for staff and pupils who have left the School are removed from the system.

**If you think your password may have been compromised or someone else has become aware of your password report this to your Computing support team via email at WillowbrookICT@outlook.com**

**Password Security**

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security
- Users are provided with an individual network, Learning Platform and Management Information System (where appropriate) log-in username
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically; individual staff users must also make sure that workstations are not left unattended and are locked
- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)

**Zombie Accounts**

Zombie accounts refers to accounts belonging to users who have left the school and therefore who no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

The school will:

- Ensure that all user accounts are disabled once the member of the school has left
- Take prompt action on disabling accounts to prevent unauthorized access

## Personal Information Promise

The Information Commissioner's Office launched a Personal Information Promise in January 2009. We have signed up to this promise which is shown below.

**The personal information promise is:**

I, Headteacher, on behalf of Willowbrook Primary School promise that we will:

1. value the personal information entrusted to us and make sure we respect that trust;
2. go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
3. consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
4. be open with individuals about how we use their information and who we give it to;
5. make it easy for individuals to access and correct their personal information;
6. keep personal information to the minimum necessary and delete it when we no longer need it;
7. have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
8. provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
9. put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
10. regularly check that we are living up to our promises and report on how we are doing

**More information available -**

**To view the promise**
https://ico.org.uk/for-organisations/improve-your-practices/personal-information-promise/

## Personal or Sensitive Information

### Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

### Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

## Remote Access

- We are responsible for all activity via our remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to School systems, keep all dial-up access information such as telephone numbers and logon IDs confidential and do not disclose them to anyone
- Select any PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

## Safe Use of Images

### Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images and videos by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device

### Publishing Pupils' Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos/videos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes

- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

**Storage of Images**

- Images/ films of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network

**Webcams and CCTV**

- The school uses CCTV for security and safety. The only people with access to this are the Office staff. We do not use publicly accessible webcams in school
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
    - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images

## School Computing Equipment including Portable & Mobile Computing Equipment & Removable Media

### School Computing Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's Computing equipment provided to you
- It is recommended that schools log equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their Computing hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available
- Ensure that all equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles
- On termination of employment, resignation or transfer, return all equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the Inclusion Manager. The Inclusion Manager is responsible for:
    - maintaining control of the allocation
    - recovering and returning equipment when no longer needed
- All redundant Computing equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

**Portable & Mobile Computing Equipment**

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile Computing equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the IT support team and fully licensed
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

**Mobile Technologies**

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

***Personal Mobile Devices (including phones)***

- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device. This will only be allowed with the approval of the class teacher in discussion with the Computing manager

***School Provided Mobile Devices (including phones)***

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community

- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

**Removable Media**

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section 'Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media'.

- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by the IT support team

**Servers**

- Newly installed servers holding personal data should be encrypted, therefore password protecting data. SIMs Database Servers are supplied with encryption software

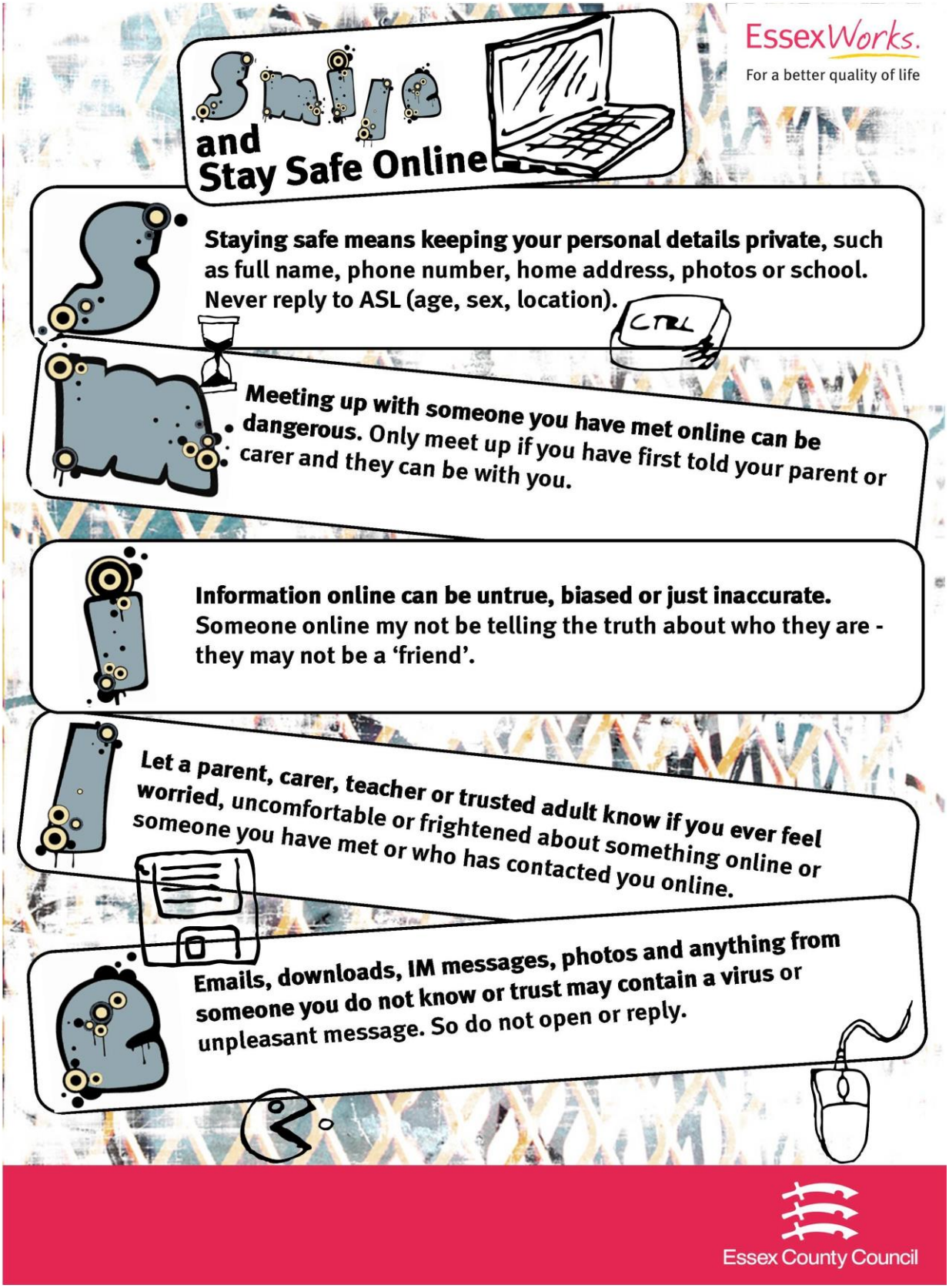
- Always keep servers in a locked and secure environment

- Limit access rights to ensure the integrity of the standard build

- Always password protect and lock the server

- Existing servers should have security software installed appropriate to the machine's specification

- Back up tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Back up tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure
- Remote back ups should be automatically securely encrypted.
- Regular updates of anti-virus and anti-spyware should be applied






Responsible person: Lisa McAdams
Adopted: May 2016
Review: May 2019
Willowbrook Primary

**Systems and Access**

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school Computing equipment or your own PC
- Do not allow any unauthorised person to use school Computing facilities and services that have been provided to you
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school Computing any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or ECC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing of the data.

## Telephone Services

- You may make or receive personal telephone calls provided:

    1. They are infrequent, kept as brief as possible and do not cause annoyance to others
    2. They are not for profit or to premium rate services
    3. They conform to this and other relevant ECC and school policies.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask your unit manager

## Writing and Reviewing this Policy

### Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety Co-ordinator any issue of eSafety that concerns them.

There will be an on-going opportunity for staff to discuss with the SIRO/AIO any issue of data security that concerns them.

This policy will be reviewed every 3 years and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

## Current Legislation

**Acts Relating to Monitoring of Staff eMail**

***Data Protection Act 1998***

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

https://www.gov.uk/data-protection/the-data-protection-act

***The Telecommunications (Lawful Business Practice)***

***(Interception of Communications) Regulations 2000***

http://www.legislation.gov.uk/uksi/2000/2699/contents/made

***Regulation of Investigatory Powers Act 2000***

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.legislation.gov.uk/ukpga/2000/23

***Human Rights Act 1998***

http://www.legislation.gov.uk/ukpga/1998/42/contents

**Other Acts Relating to eSafety**

***Racial and Religious Hatred Act 2006***

It a criminal offence to threaten people because of their faith; or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

***Sexual Offences Act 2003***

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at

least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

***Communications Act 2003 (section 127)***

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

***The Computer Misuse Act 1990 (sections 1 – 3)***

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

***Malicious Communications Act 1988 (section 1)***

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

***Copyright, Design and Patents Act 1988***

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

***Public Order Act 1986 (sections 17 – 29)***

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

***Protection of Children Act 1978 (Section 1)***

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

***Obscene Publications Act 1959 and 1964***

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

***Protection from Harassment Act 1997***

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

**Acts Relating to the Protection of Personal Data**

***Data Protection Act 1998***

https://www.gov.uk/data-protection/the-data-protection-act

***The Freedom of Information Act 2000***

http://www.legislation.gov.uk/ukpga/2000/36/contents

We acknowledge and thank Hertfordshire County Council and Essex County Council for their help in producing this model policy.