HEARTS ACADEMY TRUST

On-line Safety and Data Security Policy

Adopted by Directors: **October 2018**
To be Reviewed: **May 2021**

HEARTS Academy Trust is committed to providing a happy, caring and safe learning environment for all within a values led context, where everyone feels valued and grows in confidence and independence.

We promote HAPPINESS through a creative, exciting and practical curriculum, which generates a love of, and interest in, learning and a resilience and hope which supports us through challenging times.

Great value is placed on pupils' self ESTEEM which is developed through a positive and motivated attitude to learning, a healthy lifestyle, good social skills, self-discipline and a positive self-image.

We promote the highest standards of ACHIEVEMENT in all areas of the curriculum and help all pupils to fulfil their potential regardless of gender, race or ability.

We foster RESPECT and RESPONSIBILITY for all by establishing good relations between the school, home and community. Pupils are taught respect for themselves, others and the environment. They are also taught to take full responsibility for their own choices and responsibility for themselves and their community.

We encourage TRUTH and honesty in all aspects of school life – relationships, work and the curriculum and learn to trust and accept others' individuality and uniqueness.

We develop SPIRITUALITY and SERVICE so that calm, quiet, reflective times which support deep thought are part of school life and beauty is appreciated. We promote a service culture that reflects our duty to support and show compassion to all members of the community and not just ourselves.

Children at the heart

CONTENTS

Hearts Academy recognises that ICT and Computing are essential resources to support and enhance learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. We aim to build on the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing 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
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Green screening equipment
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

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.

The school understands the responsibility to educate our pupils about on-line 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 the 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 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

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

Breaches

A breach or suspected breach of policy by a School employee, student, 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 by an adult is grounds for disciplinary action in accordance with the Trust Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

To investigate a breach, contact support@exa.net.uk with the IP address of the machine, date and timeframe involved requesting a report form.

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 Head of School. 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 your Head of School.

See flowcharts on pages 32 for dealing with both illegal and non-illegal incidents

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB) 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 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 your 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

Data Security

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

Staff are expected to be familiar with 'Keeping children safe in education' 2018

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 ICT Acceptable Use

- 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 carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your 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. This is particularly important when shared devices (multi-function print, fax, scan and copiers) are used

Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent using the Safe Haven Fax procedure below:

Safe Haven Fax procedures

When sending personally identifiable information:

- ensure the recipient knows the fax is being sent.
- ensure the fax will be collected at the other end.
- send the front sheet through first.
- check that it has been received by the correct recipient.
- add the rest of the document to the fax.
- press the **redial** button.
- don't walk away while transmitting.
- wait for the original to process and remove it from the fax machine.
- wait for confirmation of successful transmission.
- confirm whether it is appropriate to fax to another colleague if they are not there to receive it.
- use only the minimum information and anonymise where possible

Impact Levels and Protective Marking

- Appropriate labelling of data can be used to secure data and so reduce the risk of security incidents
- Most learner or staff personal data will be classed as Protect, although some data e.g. Child Protection data, should be classed as Restricted.
- Protect/Restrict and caveat classifications that schools may use are;

  - PROTECT – PERSONAL e.g. personal information about an individual
  - PROTECT – APPOINTMENTS e.g. to be used for information about visits from the Queen or government ministers
  - PROTECT – LOCSEN e.g. for local sensitive information
  - PROTECT – STAFF e.g. Organisational staff only
  - RESTRICTED e.g. sensitive personal information about an individual

- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business
- The protective mark should be in bold capital letters within the header and footer of each page of a document
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset
- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency only. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

- All redundant ICT 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. We will only use authorised companies who will supply a written guarantee that this will happen

- Disposal of any ICT equipment will conform to regulations.

- 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

- The school gives all staff their own e-mail account to use for all school business as a work based tool This is to 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

- Under no circumstances should staff contact pupils, parents or conduct any school business 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

- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the relevant Headteacher, line manager or designated account

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

- E-mails created or received as part of your employment will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000 and the GDPR 2018. 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

- The forwarding of chain letters is not permitted in school.

- 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

- Staff must inform their line manager if they receive an offensive e-mail

- Pupils are introduced to e-mail as part of the ICT 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

- All schools in the Trust use Office 365 for the sending, receiving and organising of emails. The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending, reading or receiving business related e-mail is not permitted

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.

- 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

- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail

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

Receiving e-Mails

- Check your e-mail regularly

- Activate your 'out-of-office' notification during school closures

- Never open attachments from an untrusted source

- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

- The automatic forwarding and deletion of e-mails is not allowed

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
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted

- 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 anybody/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
- Where possible, use identifying numbers (eg payroll no) or initials instead of personal information

In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies, eg Social Care

When sending an e-mail containing personal or sensitive data you need to put a security classification in the first line of the e-mail. For e-mails to do with information about a pupil, for example, you need to put in **PROTECT – PERSONAL** on the first line of the e-mail.

This also needs to go on the top and bottom of any documents that you send (i.e. Word documents, Reports, Forms, including paper documents you send in hardcopy, etc). The name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security.

Pupils with Additional Needs

The Trust endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' online safety 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 online safety issues.

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

On-line Safety - Roles and Responsibilities

As on-line safety is an important aspect of strategic leadership within the school, the Head and Trustees have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The Trust ensures that it's CEOP ambassadors keep abreast of current issues and guidance.

Senior Management and the Local Advisory Board are updated by the Head/CEOP ambassador and the Local Advisory Board has 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, Health, Safety and Wellbeing, Behaviour/anti-bullying/exclusion and PSHE .

On-line Safety in the Curriculum

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

- The school provides opportunities within a range of curriculum areas to teach about on-line safety
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the on-line 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 and respecting other people's information, images, etc through discussion, modeling and activities
- Pupils are aware of the impact of on-line 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 Childline or the 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 on-line safety Skills Development for Staff
- Our staff receive regular information and training on-line safety issues in the form of training events, including CEOP training.
- 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 Online safety 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 expected to incorporate Online safety activities and awareness within their curriculum areas

Managing the School Online safety Messages

- We will embed online safety messages across the curriculum whenever the internet and/or related technologies are used
- The online safety policy will be introduced to the pupils at the start of each school year and continuously throughout the year

- Online safety posters will be prominently displayed

Online safety Incident Log

Some incidents may need to be recorded in other places, if they relate to a bullying or racist incident. See appendix on page 14.

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.

Managing the Internet

- The school monitors students who will 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
- 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

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
- Do not reveal names of colleagues, children or others within the school community or any other confidential information acquired through your job on any social networking site or blog
- On-line gambling or gaming 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

- The school uses broadband provision supplied by Exa, who have a monitoring solution
- School internet access is controlled through the Exa's web filtering service. Further information relating to filtering can be obtained from support@exa.net.uk

- The school is aware of its responsibility when monitoring staff communication under current legislation

- 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 teacher/Headteacher 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

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems.

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher

- 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, such as Wikipedia, YouTube, Flickr, 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 to the school

- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using systems approved by the Headteacher

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss online safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT 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 of their child being taken/ used in the public domain (e.g., on school website)

- The school disseminates information to parents relating to online safety where appropriate in the form of;

    - Information and celebration evenings
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items
    - Learning platform training
    - Parent workshops

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 regularly and 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 ICT 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 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 ICT support team

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, email, Learning Platform and Management Information System (where appropriate) log-in username. They are also expected to use a personal password and keep it private
- 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)
- All staff and pupils are expected to comply with the policies at all times

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore 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.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorised access
- Regularly change generic passwords to avoid unauthorised access (Microsoft© advise every 42 days)

Further advice available http://www.itgovernance.co.uk/

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 devices/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

- You are responsible for all activity via your remote access facility

- Only use equipment with an appropriate level of security for remote access
- Select 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

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.

- Parents and Staff are encouraged to write to the school if they do not give permission for the appropriate taking of images 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 Pupil's Images and Work

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

- on the school website
- on the school's internet media, ieYoutube channel, Facebook page
- on the school's Learning Platform
- 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 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. Parents/ carers may withdraw permission, in writing, at any time.

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

Only the Web Manager has authority to upload to the site or disseminate this responsibility to a named person.

Storage of Images

- Images/ films of children are only 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. These must not be removed from the school site

- The staff member who saved the images has the responsibility of deleting them when they are no longer required, or the pupil has left the school

Webcams

- We do not use publicly accessible webcams in school

- Webcams in school are only ever used for specific learning purposes, i.e. Iris, monitoring hens' eggs, recording sample lessons, CPD, drama etc

- Misuse of a webcam by any member of the school community will result in sanctions

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school

- All pupils are supervised by a member of staff when video conferencing

- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school

- The school keeps a record of video conferences, including date, time and participants.

- Approval from the Headteacher is sought prior to all video conferences within school

- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences

- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked

- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you

- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory

- Do not allow your visitors to plug their ICT 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 ICT 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

- Privately owned ICT equipment should not be used on a school network

- On termination of employment, resignation or transfer, return all ICT 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 appropriate Line Manager. Authorising Managers are responsible for:

    - maintaining control of the allocation and transfer within their Unit
    - recovering and returning equipment when no longer needed

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT 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 ICT 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 ICT support team, fully licensed and only carried out by your ICT support

- 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 and 1:1 device ownership 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 allows staff to bring in personal mobile phones and devices, but they must be switched on silent and out of use during the school day. Only in exceptional circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device but this must be done so with the private number being withheld.

- Pupils are allowed to bring personal mobile devices/phones to school but they must be kept securely in the school office. At all times the device must be switched off.

- The school is not responsible for the loss, damage or theft of any personal mobile device

- The sending of inappropriate text messages or images 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

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages/images 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

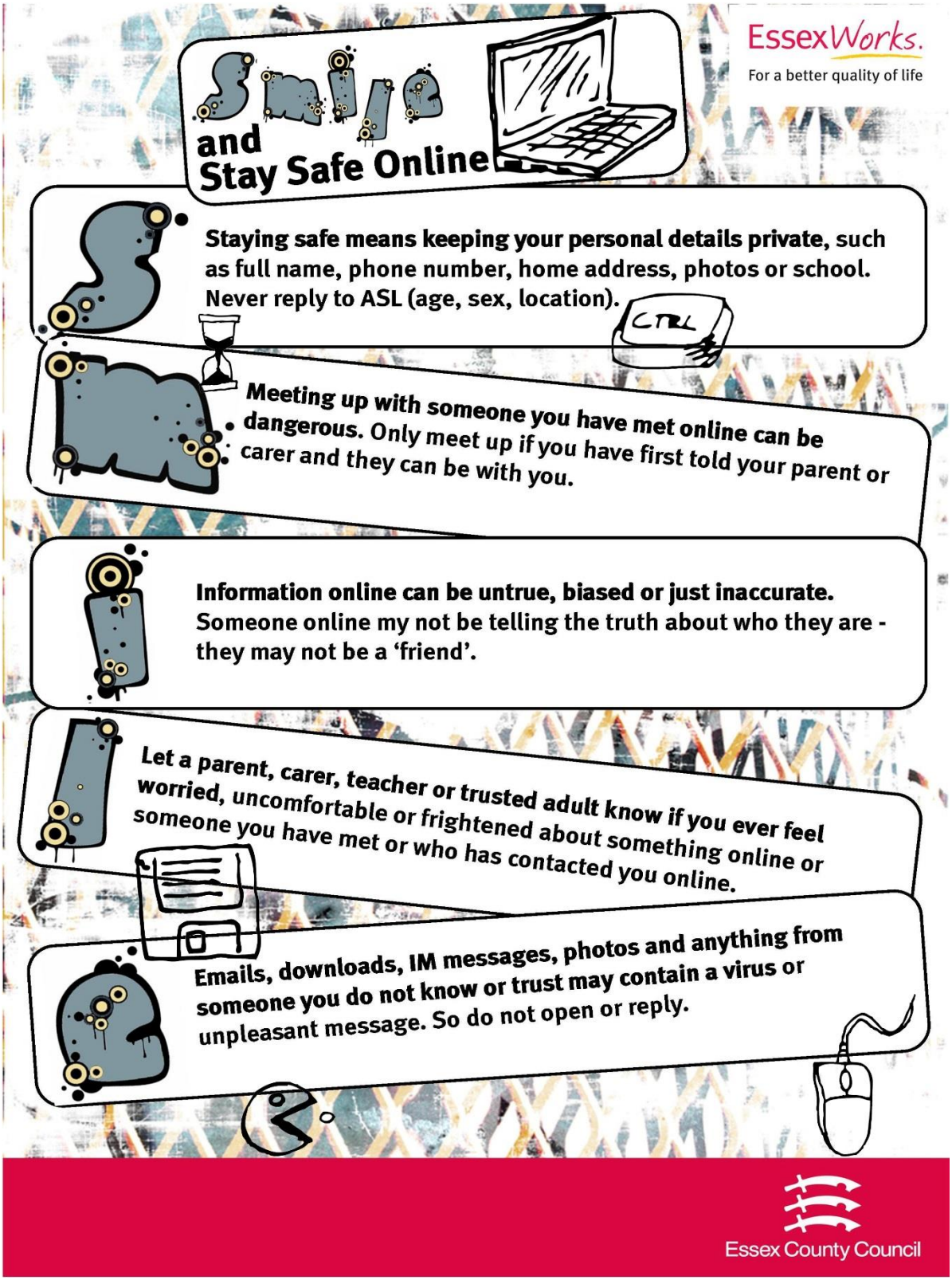
- Only use recommended removable media
- Do not store sensitive information on removable media
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

Servers

- Newly installed servers holding personal data should be encrypted, therefore password protecting data.

- 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 backups should be automatically securely encrypted.
- Regular updates of anti-virus and anti-spyware should be applied
- Records should be kept detailing when and which patches have been applied


Smile
and
Stay Safe Online
EssexWorks.
For a better quality of life
Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location).
CTRL
Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.
Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'.
Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.
Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.
Essex County Council

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 ICT equipment or your own PC

- Do not allow any unauthorised person to use school ICT 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 ICT 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 Trust 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 and a Subject Access Request.

- 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:

  They are infrequent, kept as brief as possible and do not cause annoyance to others
  They are not for profit or to premium rate services
  They conform to this and other relevant 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

- Ensure that your incoming telephone calls can be handled at all times

- 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 manager

Acceptable Use Agreement: Pupils - Primary

Primary Pupil Acceptable Use Agreement/Online safety Rules

- I will only use ICT in school for school purposes.
- 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 tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- 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.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my online safety.
- I will not hold a personal account on/ or access social media networking sites, e.g. Facebook, snapchat, etc.

School logo and details

Dear Parent/Carer

ICT including the internet, e-mail and mobile technologies, etc has become an important part of learning in our school.   We expect all children to be safe and responsible when using any ICT.

Please read and discuss these online safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact the school office.

This Acceptable Use Agreement is a summary of our online safety Policy which is available in full via our publications scheme on request.

Parent/Carer signature

We have discussed this and ……………………………………...........(child name) agrees to follow the online safety rules and to support the safe use of ICT at the School.

Parent/Carer Signature ………………………………………………….

Class ………………………………… Date ………………………………

Acceptable Use Agreement/Code of Conduct

IT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in education. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Penny Partridge, Trust Business Manager.

- I will only use the Trust's email/internet/learning platform and any related technologies for professional purposes or for use deemed 'reasonable' by the Heads of Schools, Executive Headteacher or Governing Body.
- I will comply with the IT system security and not disclose any passwords provided to me by the Trust, schools or other related authorities.
- I will ensure that all electronic communications with stakeholders, pupils and staff are compatible with my professional role.
- I will not give out my personal details, such as mobile phone number, personal e-mail address and social networking identities to pupils.
- I will ensure that personal data (such as data held on MIS software) 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 of School or Local Advisory Board. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware without permission of the Head of School.
- 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 in line with Trust 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 Head of School.
- 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 my line manager or Heads of Schools.
- 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 Trust's online safety and data Security policies and help pupils to be safe and responsible in their use of IT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

This Acceptable Use Agreement is a summary of our online safety Policy which is available on request or on our website

User signature

I agree to follow this code of conduct and to support the safe and secure use of IT throughout the Trust

Full name: _____

Signature: _____

Job title: _____

Date: _____

e-Safety Incident Log

Details of ALL e-Safety incidents to be recorded by the Headteacher. This incident log will be monitored termly by the Headteacher, Member of SLT or Local Advisory Board.

Complaints

Complaints and/ or issues relating to Online safety should be made to the Headteacher. Incidents should be logged and the **Flowcharts for Managing an Online safety 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 Headteacher
- Deliberate access to inappropriate materials by any user will lead to the incident being logged, and depending on the seriousness of the offence; investigated with the possibility of immediate suspension leading to dismissal and involvement of police for very serious offences (see flowchart)

Date & Time	Name of pupil or staff member	Room and computer/device number	Details of incident (including evidence)	Actions and reasons

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

The Headteacher/e-Safety Co-ordinator should:
- **Record the incident in the e-safety log**
- **Keep any evidence**

Did the incident involve a member ofstaff?

YES

If a member of staff has:
1. Behaved in a way that has, or may have, harmed a child
2. Possibly committed a criminal offence
3. Behaved towards a child in a way that indicates that s/he may be unsuitable to work with children Contact LADO on **03330 139 797**

- Review evidence and determine whether the incident was accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures

NO

Was the Child the victim orperpetrato

Pupil asVictim

Support the pupil by one or more of the following:
- Class Teacher
- e-Safety Co-ordinator
- Headteacher/Senior Leader
- Designated Child Protection Officer
- School PCSO

Inform Parent/carer as appropriate
If the child is at risk contact Social Care Direct to make an emergency referral on **0345 603 7627**

Pupil as Instigator

Incident types could be:
- Using another persons user name or password
- Accessing websites which are against the schools policy e.g. gaming
- Using a mobile phone to take video during a lesson
- Using technology to upset or bully

- Review incident to decide if other pupils were involved
- Decide appropriate sanctions
- Inform Parent/Carer if serious or persistent incident
- If serious, consider informing the Duty Safeguarding Officer as the child instigator could be at risk

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

Following an e-safety incident a decision will have to be made quickly as to whether the incident involved any illegal activity

Has illegal activity taken

YES

NO

Examples of illegal activity would include:
- Downloading abusive images
- Passing child pornography to others
- Inciting racist or religious hatred
- Extreme cases of cyberbullying

Still unsure?

For further advice ECC ISIS helpdesk on 01245 431851 or Essex Police on 0300 333 4444

- ✓ Inform Essex Police and Essex County Council
- ✓ Follow the advice given by the Police, or
- ✓ Confiscate the device and if related to the school network disable user account
- ✓ Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence
- ✓ If a pupil is involved contact Social Care Direct to make an emergency referral on 0845 603 7627
- ✓ If it involves a member of staffcontact the LADO on 03330 139 797.

Go to the flowchart which outlines the process for non-illegal incidents

Users must be aware that if they find something unpleasant or frightening they should switch off their screen or close the laptop and talk to a member of staff

Further information

Information Commissioner website
https://ico.org.uk/

Data Protection Act – data protection guide, including the 8 principles
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

IT Guidance
http://www.itgovernance.co.uk/

CEOP

https://www.ceop.police.uk/safety-centre/

Parent Info
http://parentinfo.org/

NSPCC Net Aware
https://www.net-aware.org.uk/

Talking pants online
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/

Internet Matters
https://www.internetmatters.org/issues/cyberbullying/

Keeping Children Safe in Education
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2