ALAMEDA MIDDLE SCHOOL

INSPIRE • ACHIEVE • EXCEL

e-SAFETY POLICY

DOCUMENT STATUS

ORIGINAL AUTHOR	Maxine Warner
DATE OF PRODUCTION	February 2018February 2018
CURRENT STATUS	Approved
REVIEWING BODY	Resources Committee
REVIEWED ON	February 2018
DATE FOR NEXT REVIEW	2021
RELATED POLICIES (IF ANY)	Behaviour

TABLE OF CONTENTS

1. RATIONALE

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

ICT covers a broad range of resources and technologies and this is changing at a rapid pace and it is important to recognise the ubiquity of technology within society as a whole. The presence of technology in so many aspects of our lives means that we must embrace it and foster good and safe use. 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
- Email and Instant Messaging
- Chat Rooms
- Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming

These technologies are accessed through a variety of devices including PCs, laptops, tablets, smart phones and smart TVs and with more and more devices becoming internet enabled the number of access mechanisms is constantly increasing.

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 technologies and to learn how to use them both effectively and safely.

At Alameda Middle School, we understand the responsibility to educate our pupils on eSafety issues and to teach 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.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of all technology used to access resources whether these are technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc) or technologies owned by pupils and staff, but brought onto school premises (such as laptops, tablets,smart phones, or portable media players, etc).

Parents/ carers are asked to read through and sign acceptable use agreements with their child on admission to the school. An updated copy of the agreement will be reproduced annually in the Home/School diary and should also be signed on an annual basis.

The school disseminates information to parents relating to eSafety where appropriate in the form of;

- Information and celebration evenings
- Posters
- Website postings
- Newsletter items

2. 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 our school is the head. 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 as the LA, CEOP (Child Exploitation and Online Protection) and Childnet.

The Senior Leadership Team and Governors are updated by the 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 (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: safeguarding policy, health and safety policy, behaviour policy, anti-bullying policy and the PHSE policy.

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's eSafety Policy. (Appendix 1 for staff, Appendix 2 for pupils).

3. MANAGING THE SCHOOL ESAFETY MESSAGES

- We endeavour to embed eSafety messages across the curriculum whenever internet connected technologies are used and to relate these to outside examples where appropriate to convey the message that vigilance is required at all times when using internet connected technology
- The eSafety policy will be introduced to the pupils at the start of each school year.
- E-safety posters will be prominently displayed.
- Impero monitoring software is set up to enforce a digital signature from all pupils logging into a monitored computer on the network for the first time. This shows an acceptable use policy and accepts their click as agreed. This is logged for all pupils.

4. ESAFETY SKILLS DEVELOPMENT FOR STAFF

- Staff will receive regular information and training on eSafety issues as new developments occur; All staff will be expected to incorporate eSafety activities and awareness within their curriculum areas.
- 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 attached flowchart.)

5. ESAFETY IN THE CURRICULUM

- The school provides opportunities within a range of curriculum areas to teach about eSafety (Computing and Values/PSHCE).
- 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, modelling and activities.
- Pupils are aware of how their behaviour can affect others and the impact of having their behaviour reported.
- Pupils are made aware that everything they place on the internet in any form will never be deleted and can impact them in the future
- Pupils are made aware that anything they post of the internet may be viewed by anybody unless they take appropriate privacy precautions
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. 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/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teaching and via the ICT curriculum.

6. PASSWORD SECURITY

- Users are provided with an individual network and Learning Platform log-in username. They are expected to use a personal password and to keep it private.
- Users who believe that their password may have been compromised or someone else has become aware of their password should report this to their teacher (if a pupil), or to the network manager (if a staff member).
- Pupils are not allowed to use the accounts of others, or make any attempt to 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 Learning Platform, including ensuring that passwords are not shared.Individual staff users must also make sure that workstations are not left unattended without being locked.
- The system requires staff to change their passwords once every term.
- Pupils and staff must ensure that they log off the school network at the end of each lesson, or at the end of each day.
- Password cannot be saved in the cache when logging on to the learning platform on any computer which is shared (this is disabled).

7. DATA SECURITY

It is a legal requirement of the Data Protection Act 1998 to protect and secure personal data. This is defined as "any combination of data items that identifies an individual and gives specific information about them, their families or circumstances. This includes names, contact details, gender, dates of birth, behaviour and assessment records."

The advent of the European General Data Protection Regulation will require more stringent protection of this data and the school are actively ensuring that compliance with this new legislation will be in place by May 2018.

Staff should follow the procedures outlined in Appendix 3 –Data Security Do's and Don'ts.

8. MANAGING THE INTERNET

The internet is an open communication medium, available to all, at all times and provides multiple communication channels, information sources and means of publishing information. This flexibility makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- Pupils will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology on equipment provided by the school.
- 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.
- 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 and network manager.
- 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 all materials from electronic resources.

9. INFRASTRUCTURE

- Alameda Middle School 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.
- School internet access is controlled through Central Bedfordshire's web filtering service provided by E2BN. These are Middle School level filters that monitor all pupil web use. This is backed up with Impero software which monitors websites using keywords linked to racism or other inappropriate searches and monitors keys typed on the keyboard.
- 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.
- eSafetyIt 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; staff with school laptops will check that updates are being regularly performed.
- Personal removable media is not permitted to be used on school equipment (including laptops) without explicit permission from the the Network Manager.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Network Manager.
- If there are any issues related to viruses or anti-virus software, the Network Manager should be informed immediately and the affected device removed immediately from the school network.No further use of that technology should be made until the issue is resolved.

10. MANAGING SOCIAL NETWORKS

Social networking sites, if used responsibly, both outside and within an educational context, can provide easy to use, creative and free facilities. However, it is important to recognise that there are risks in using such sites in respect of content, privacy and the potential for exploitation. 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 endeavours to deny access to social networking sites to pupils within school. Parents are made aware of the legal age (currently 13, soon to increase to 16) for children to access social media via items in the newsletter and on the school's Facebook page.
- 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 also warned of the additional hidden data that may be contained in images that are posted and the consequences of this additional information.
- Pupils are warned that any data posted on a social networking site may appear to have been deleted but is held in perpetuity by the site providers and should, therefore, be regarded as being there forever.
- 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, email address, specific hobbies/ interests).
- Pupils are advised not to share information on their location, especially when they are on holiday or home alone.
- 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 similar in order to communicate with pupils using the LA Learning Platform or other systems approved by the Headteacher.

- Pupils are educated on the value on social media in the context that it is an additional way of communicating but does not replace face to face conversations or spending time with friends.

11. 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, gaming devices, smart phones and tablets are familiar to some children outside of school too. They can 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:

12. PERSONAL MOBILE DEVICES (INCLUDING PHONES)

- The school does not allow pupils to have personal mobile phones and devices in lessons for use during the school day. The school does allow staff to bring in personal mobile phones and devices for their own use. The school allows a member of staff to contact a pupil or parent/carer using their personal device on school business only and advises that where possible, the school telephone system is used.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate electronic messages between any members 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.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Where the school provides mobile technologies such as phones, and laptops 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.

13. MANAGING EMAIL

The use of email is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email 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 email in relation to their age and good 'netiquette'.

- The school gives all permanent staff their own email account to use for all school business. Only these accounts should be used for school business.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all email is filtered and logged and copies of all emails sent and received are retained. This allows historical emails to be recovered even if they have been deleted from the users mailbox
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff should always consider whether email is the appropriate medium for a communication or whether a letter may be a more appropriate approach in certain circumstances.
- Staff and pupils are made aware that email communication is not transitory and that all email sent and received on the school system are logged and retained.
- All pupils have access to the messaging system allocated on the school learning platform. Only this system may be used in school and to send work or file attachments to school.
- All email and message senders are expected to adhere to the generally accepted rules of network etiquette (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 message.
- Staff must inform the eSafety co-ordinator or their line manager if they receive an offensive e-mail.
- Pupils are introduced to email and messaging as a part of their induction in the use of the school's ICT systems in year 5.

14. SAFE USE OF IMAGES

14.1. TAKING OF IMAGES AND FILM

Digital images are easy to capture, reproduce and publish and, therefore, misused. It is therefore not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering any potential harm that might arise.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Where possible and practicable, a camera or other school device will be provided for staff to use to take pictures.
- Where it is not practicable or possible to use a school owned device and with the express permission of the Headteacher, images can be taken on devices including phones owned by staff, provided they are transferred immediately to the school's network and or website/Facebook page and deleted from the staff device.
- All devices will have GPS tagging disabled and all images will be checked for hidden meta-data before being published to any public medium. No meta-data will be published with any image.
- Images will be reviewed to ensure that, wherever possible, identifying information such as school badges, location identifiers or similar elements are not present or are removed prior to publishing of an image
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file. This permission is reviewed every year as emerging technology may lead to a decision to revoke permission. At any time a staff member may request revocation of permission but this will not apply to images published prior to the revocation request.

14.2. PUBLISHING PUPIL'S IMAGES AND WORK

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

- on the school web site, Learning Platform and Facebook page.
- 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, ie exhibition promoting the school
- general media appearances, eg 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, eg divorce of parents, custody issues, etc. in which case, parents must contact the school to inform of this.

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

Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published, only initials and surnames will be used where pictures are included.

The Headteacher must authorise all web site content. This is uploaded by the designated Web editor(s).

14.3. STORAGE OF IMAGES

- Images/ films of children are stored only on the school's network Learning Platform or website and are not retained on any other device
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks, laptops) 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/ Learning Platform.

14.4. WEBCAMS AND CCTV

- The school uses CCTV for security and safety. Notification of CCTV use is displayed at the front of the school. CCTV images are securely stored and not accessible without written permission from the Headteacher.
- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes. Pupils will be supervised when using webcams.

- 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)

14.5. VIDEO CONFERENCING

- 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
- 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.
- No part of any video conference is recorded by either the school or the third party in any medium without the written consent of those taking part.
- Misuse and Infringements

15. COMPLAINTS

Complaints relating to eSafety should be made to the Headteacher. Incidents should be logged and the Flowcharts for Managing an eSafety Incident should be followed (see appendix 4).

16. INAPPROPRIATE MATERIAL

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Network Manager.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Network Manager. Depending on the seriousness of the offence, there will be an investigation by the Headteacher (or person delegated by the Headteacher), immediate suspension, possibly leading to dismissal and involvement of the police for very serious offences (see flowchart – Appendix 4)

17. EQUAL OPPORTUNITIES

17.1. 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 schools' 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.

18. STAFF, GOVERNOR, PARENT AND PUPIL INVOLVEMENT IN POLICY CREATION

18.1. REVIEW PROCEDURE

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

Staff, Governors and pupils have been involved in making/ reviewing the eSafety policy through School Council, governor and staff meetings and parents through the newsletter and parent forum. This policy will be reviewed through the same process every 6 months 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.

APPENDIX 1

STAFF, GOVERNOR AND VISITOR

ACCEPTABLE USE AGREEMENT / CODE OF CONDUCT

The school provides access to its own networked resources, and to internet resources, including the Alameda Learning Platform. Some of these resources are available from outside of school and the responsible use rules apply wherever they are used. This *Acceptable Use Agreement* is reviewed annually, and is intended to protect the whole school community by clearly stating what is acceptable and what is not.

You are asked to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the school 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 school ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will not knowingly compromise the security and smooth running of ICT systems provided by the school.
- 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 and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) 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.
- I will not install any hardware of software in school, or to school hardware without permission of the Network Manager.

- 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 where written consent of the parent, carer or staff member has been obtained. 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 my Line Manager or 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 not use public chat rooms or social networking sites within school.
- I will support and promote the school's eSafety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

USER SIGNATURE

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

SIGNATURE _____ DATE _____

FULL NAME (PLEASE PRINT) _____

JOB TITLE/ROLE _____

APPENDIX 2

PUPIL ACCEPTABLE USE AGREEMENT / ESAFETY RULES

The school provides access to its own networked resources, and to internet resources, including the Alameda Learning Platform. Some of these resources are available from outside of school and the responsible use rules apply wherever they are used. This *Acceptable Use Agreement* is reviewed annually, and is intended to protect the whole school community by clearly stating what is acceptable and what is not.

You are asked to sign this agreement and always follow the stated rules. These rules – together with any amendments - will be included in the school Homework Diary which you are asked to sign at the start of each school year. Any concerns or clarification should be discussed with the deputy head – school eSafety coordinator.

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- If I bring a phone into school I will make sure it is secured in my locker or handed in at reception throughout the school day.
- I will not bring any other personal devices (mp3 players, ipods,) into school.
- I may bring a pen drive or portable storage device into school but this must not be used on the school computers without first being security checked by a member of staff.
- I will only log on to the school network/ Learning Platform with my own user name and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.

- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I understand that images of pupils and/ or staff will only be taken, stored and used for school purposes inline with school policy and not be distributed outside the school network without the permission of the Headteacher.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring anyone into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

PUPIL AND PARENT/ CARER SIGNATURE

We have discussed this document and .....(pupil name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at Alameda Middle School.

PARENT/CARER SIGNATURE _____

PUPIL SIGNATURE _____

FORM _____ DATE _____

APPENDIX 3

GOOD PRACTICE IN INFORMATION HANDLING

The aim of this advice is to raise your awareness of where potential breaches of security could occur. Following these 'dos and don'ts' will help you to prevent data from being lost or used in a way which may cause individuals harm or distress and/or prevent the loss of reputation your organisation may suffer if you lose personal data about individuals. This was written by BECTA before its closure in 2011.

YOUR ROLES AND RESPONSIBILITIES

As a member of your organisation you have a shared responsibility to secure any sensitive or personal data you use in your day-to-day professional duties.

IMPORTANT 'DOS'

- make sure you and your colleagues are adequately trained
- follow guidance
- become more security aware
- raise any security concerns
- encourage your colleagues to follow good practice and guidance
- report incidents.

WHY PROTECT INFORMATION?

Organisations hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this data could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of personal data could result in adverse media coverage, and potentially damage the reputation of your organisation. This can make it more difficult for your organisation to use technology to benefit learners.

WHAT INFORMATION DO YOU NEED TO PROTECT?

You should secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to your organisation. Your organisation should have someone who is responsible for working out exactly what information needs to be secured. This person is your Information Asset Owner. They should understand what information you need to handle, how the information changes over time, who else is able to use it and why. Several people may share this role if you work in a large organisation.

If you don't already know, find out who is acting as your Information Asset Owner.

USING PROTECTIVE MARKINGS

It is good practice to protectively mark personal data. This will help people handling it understand the need to keep it secure and to destroy it when it is no longer needed. This is especially important if personal data information is combined into a report and printed.

Your Information Asset Owner should help you work out how you need to mark the information you view as part of your job. There are different levels of marking depending on how just how sensitive the information is.

STEPS YOU CAN TAKE TO HELP PREVENT SECURITY PROBLEMS

There are plenty of things that you should do (or not do) that will greatly reduce the risks of sensitive information going missing or being obtained illegally. Many of these 'dos and don'ts' will apply to how you handle your own personal information. Using these practices will help you to protect your own privacy.

We have separated these points into different areas to make it easier for you to refer back to.

WORKING ONLINE

DO

- make sure that you follow your organisation's policies on keeping your computers up to date with the latest security updates. Make sure that you keep any computers that you own up to

date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). Get advice from your IT team if you need help.

- only visit websites that are allowed by your organisation. Remember your organisation may monitor and record (log) the websites you visit.
- turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer and attack and forgery site warnings in Mozilla Firefox.)
- make sure that you only install software that your IT team has checked and approved
- be wary of links to websites in emails, especially if the email is unsolicited
- only download files or programs from sources you trust. If in doubt, talk to your IT team.
- check that your organisation has an acceptable-use policy (AUP) for the internet and ensure that you follow it.

EMAIL AND MESSAGING

DO

- read your organisation's email policy
- report any spam or phishing[1] emails to your IT team that are not blocked or filtered
- report phishing emails to the organisation they are supposedly from
- use your organisation's contacts or address book. This helps to stop email being sent to the wrong address.

DON'T

- click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on.
- turn off any email security measures that your IT team has put in place or recommended
- email sensitive information unless you know it is encrypted. Talk to your IT team for advice.
- try to bypass your organisation's security measures to access your email off-site (for example, forwarding email to a personal account)
- reply to chain emails

PASSWORDS

DO

- follow your organisation's password policy
- use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers)
- make your password easy to remember, but hard to guess
- choose a password that is quick to type
- use a mnemonic (such as a rhyme, acronym or phrase) to help you remember your password. Change your password(s) if you think someone may have found out what they are.

DON'T

- share your passwords with anyone else
- write your passwords down
- use your work passwords for your own personal online accounts
- save passwords in web browsers if offered to do so
- use your username as a password
- use names as passwords
- email your password or share it in an instant message.

LAPTOPS

DO

- shut down your laptop using the 'Shut Down' or 'Turn Off' option
- try to prevent people from watching you enter passwords or view sensitive information
- turn off and store your laptop securely (if travelling, use your hotel's safe)
- use a physical laptop lock if available to prevent theft
- lock your desktop when leaving your laptop unattended
- make sure your laptop is protected with encryption software.

DON'T

- store remote access tokens with your laptop
- leave your laptop unattended unless you trust the physical security in place
- use public wireless hotspots – they are not secure
- leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
- let unauthorised people use your laptop
- use hibernate or standby.

SENDING AND SHARING

DO

- be aware of who you are allowed to share information with. Check with your Information Asset Owner if you are not sure.
- ask third parties how they will protect sensitive information once it has been passed to them
- encrypt all removable media (USB pen drives, CDs, portable drives) taken outside your organisation or sent by post or courier.

DON'T

- send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives) if secure remote access is available
- send sensitive information by email unless it is encrypted
- place protective labels on outside envelopes. Use an inner envelope if necessary. This means that people can't see from the outside that the envelope contains sensitive information.
- assume that third-party organisations know how your information should be protected.

WORKING ON-SITE

DO

- lock sensitive information away when left unattended
- use a lock for your laptop to help prevent opportunistic theft.

DON'T

- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room.

WORKING OFF-SITE

DO

- only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above.
- wherever possible access data remotely instead of taking it off-site
- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any services you have used
- try to reduce the risk of people looking at what you are working with
- leave your laptop behind if you travel abroad (some countries restrict or prohibit encryption technologies).

APPENDIX 5

ALAMEDA ESAFETY INCIDENT LOG

Details of ALL eSafety incidents are to be recorded by the Network Manager. This incident log will be monitored termly by the Headteacher, member of SLT or Chair of Governors. Any incidents involving cyber bullying should be recorded using the behaviour monitoring system.

Date and Time	Name of pupil or staff member	Male/female	Room and computer/device no.	Details of incident	Actions and reasons

APPENDIX 6

SMILE AND STAY SAFE POSTER

E-Safety Rules to be displayed next to all PCs in school

and stay safe

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)

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.

APPENDIX 7

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.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

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.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

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.

For more information

www.teachernet.gov.uk

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 a 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.