Moulsham Junior School

E-Safety Policy

Reviewed with Staff: Summer Term 2016
Ratified by Governors: Summer Term 2016
Next review: Summer Term 2018

Moulsham Junior School

E-safety

and

Data Security

Guidance Policies for Computing
Acceptable Use

Author: Angela Holden, Computing Subject Leader

Date of issue: May 2016

Review date: May 2016

CONTENTS

Introduction

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

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

Whilst exciting and beneficial both in and out of the context of education, much Computing, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Moulsham Junior School**,** we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

As part of e-safety within Moulsham Juniors, our pupils, parents and staff are expected to follow acceptable use agreements (see Appendices B, C, D and E).

Monitoring

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

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

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

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

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

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School Computing hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the Essex County Council Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of Computing must be immediately reported to the school's e-safety co- ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, misuse or unauthorised use of Computing and all other policy non-compliance must be reported to your e-safety co- ordinator.

Data Security

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

The school follows Becta guidelines http://webarchive.nationalarchives.gov.uk/20110130111510/http:/schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734 published Spring 2009) and the Local Authority guidance documents listed below

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

Teachers and Governors Guidance (2012) https://ico.org.uk/media/for-organisations/documents/1132/report_dp_guidance_for_schools.pdf

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

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
- Leadership have identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO)
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile Computing 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 Computing equipment or removable media as hand luggage, and keep it under your control at all time

- 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 copiers (multi-function print, fax, scan and copiers) are used

E-Safety Officer

The officer is a senior member of staff who is familiar with information risks and the school's response. The officer should have the following responsibilities:

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

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support officers in their role.
The officer in this school is Angela Holden.

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Schools should identify an Information Asset Owner. For example, the school's Management Information System (MIS) should be identified as an asset and should have an Information Asset Owner. In this example the MIS Administrator or Manager could be the IAO.

The role of an IAO is to understand:

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

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

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

The officer in this school for staff is Mark Cresswell. The officer in this school for pupil data is Mark Cresswell.

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
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder
- 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 School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform e-safety co-ordinator if they receive an offensive e-mail

e-safety

e-safety in the Curriculum

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

- The school has a framework for teaching internet skills in Computing / PSHE lessons
- The school provides opportunities within a range of curriculum areas to teach about e-safety
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.

E-safety Skills Development for Staff

- Our staff receive regular information and training on e-safety issues through staff meetings and inset days
- 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 e-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 e-safety activities and awareness within their curriculum areas

Incident Reporting, e-safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of Computing must be immediately reported to the school's e-safety co- ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of Computing and all other policy non-compliance must be reported to your e-safety Co-ordinator.

Misuse and Infringements

Complaints

Complaints and/ or issues relating to e-safety should be made to the e-safety co-ordinator or Headteacher. Incidents should be logged and the **Essex Flowcharts for Managing an e-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 e-safety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart – Appendix A)
- Users are made aware of sanctions relating to the misuse or misconduct through the 'Acceptable User Agreement.'

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. All use of the **Essex Grid for Learning** (EGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The school maintains 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

Validity of Information

We believe that, in order to use information from the internet effectively, it is important for pupils to develop an understanding of the nature of how the internet and the information available on it. In particular, they should know that, unlike the school library for example, most of the information on the internet is intended for an adult audience, much of the information on the internet is not properly audited/edited and most of it is copyright.

- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV
- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium)
- Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

Internet Use

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

- Essex County Council has a monitoring solution via the Essex Grid for Learning where web-based activity is monitored and recorded
- Due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that particular types of material will neve reappear on a computer screen. Neither the school nor ECC can accept liability for the material accessed, or any consequences thereof.
- School internet access is controlled through the LA's web filtering service. For further information relating to filtering please go to essexcc-servicedesk.sen.uk@siemens-enterprise.com
- Moulsham Junior 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
- It is the responsibility of the school, by delegation to the Computing technician, 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 Computing technician 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 technician or Computing subject leader.
- If there are any issues related to viruses or anti-virus software, the Computing technician should be informed

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure
- Ensure 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 copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

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

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

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to School systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- 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

Current Legislation

This policy reflects and makes reference to the following current legislation:

Data Protection Act 1998
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
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Racial and Religious Hatred Act 2006
http://www.legislation.gov.uk/ukpga/2006/1/pdfs/ukpga_20060001_en.pdf

Sexual Offences Act 2003
http://www.legislation.gov.uk/ukpga/2003/42/contents

Communications Act 2003 (section 127)
http://www.legislation.gov.uk/ukpga/2003/21/section/127

The Computer Misuse Act 1990 (sections 1 – 3)
http://www.legislation.gov.uk/ukpga/1990/18/section/1

Malicious Communications Act 1988 (section 1)
http://www.legislation.gov.uk/ukpga/1988/27/section/1

Copyright, Design and Patents Act 1988
http://www.legislation.gov.uk/ukpga/1988/48/contents

Public Order Act 1986 (sections 17 – 29)
http://www.legislation.gov.uk/ukpga/1986/64/contents

Protection of Children Act 1978 (Section 1)
http://www.legislation.gov.uk/ukpga/1978/37/pdfs/ukpga_19780037_en.pdf

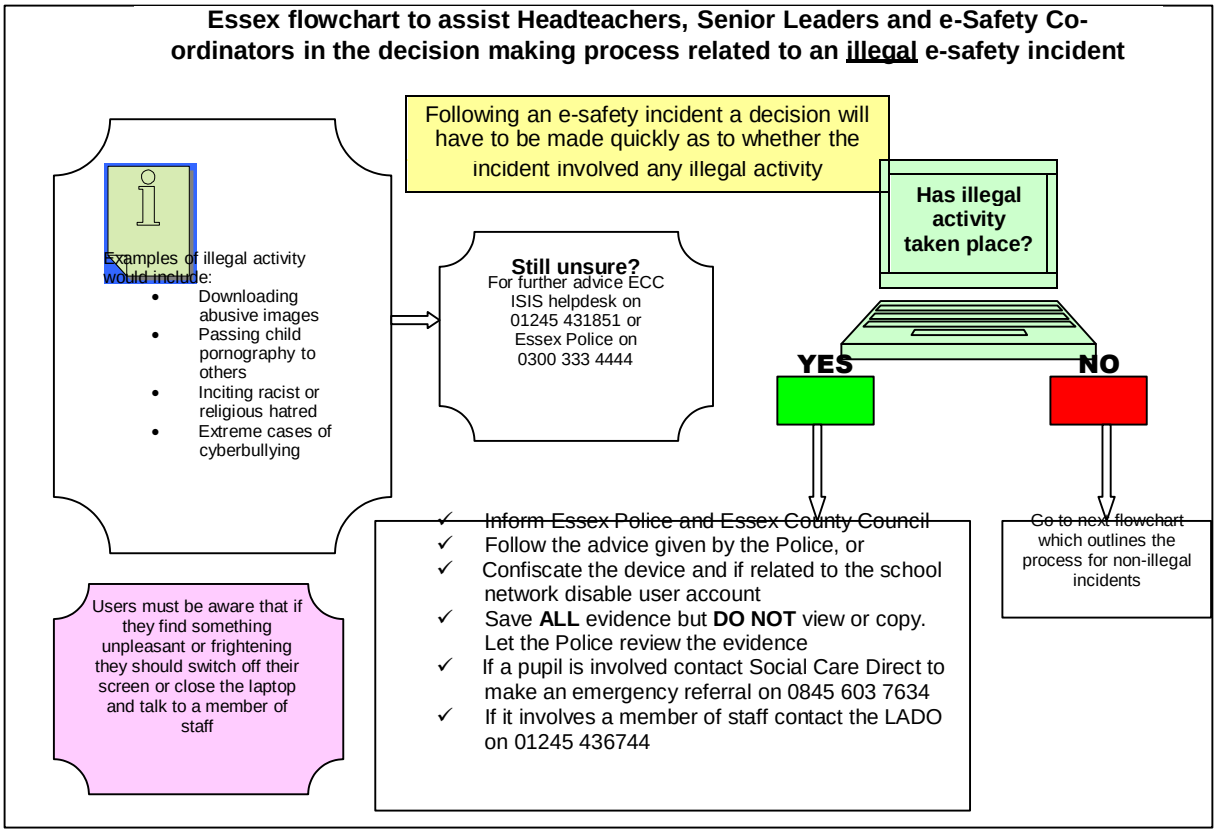
Obscene Publications Act 1959 and 1964
http://www.legislation.gov.uk/ukpga/1964/74

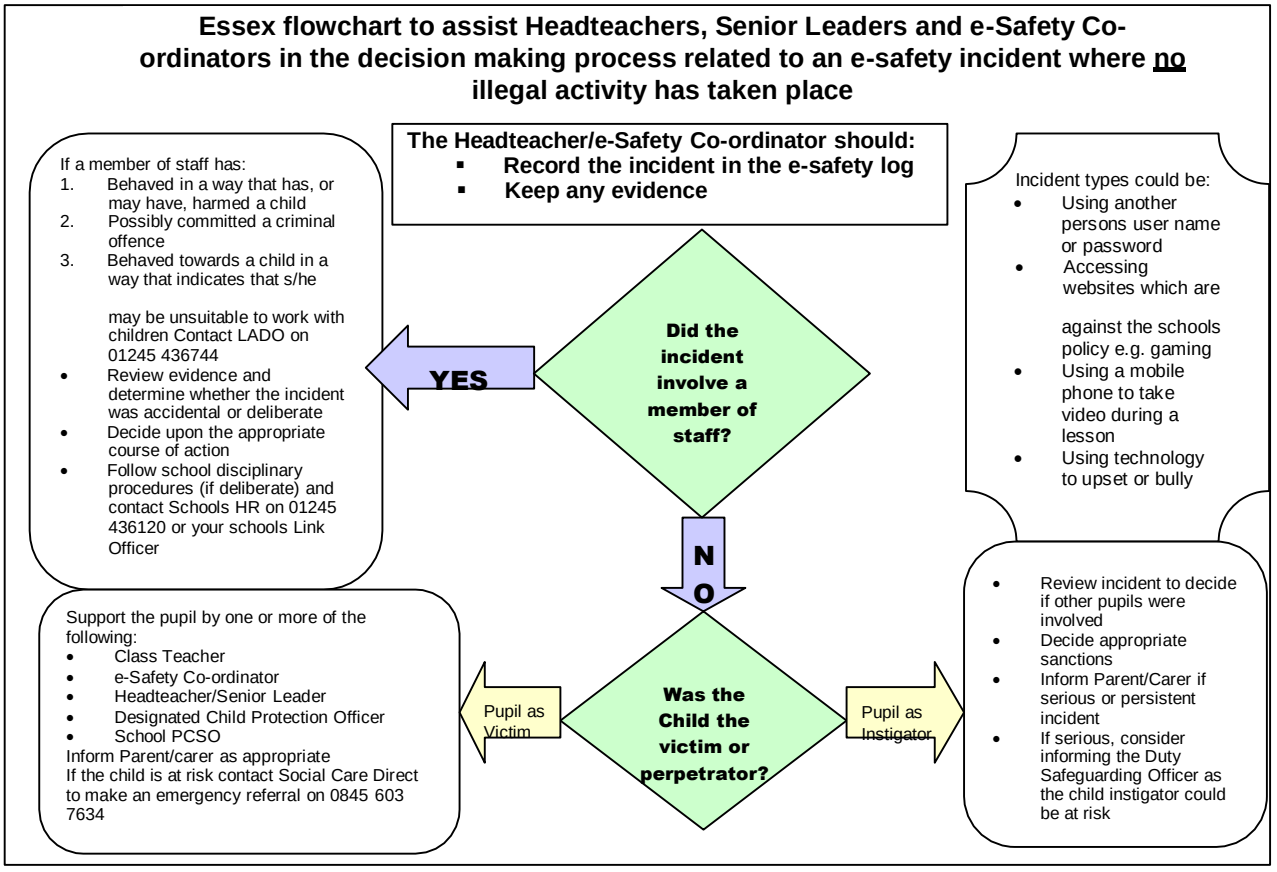
Protection from Harassment Act 1997
http://www.legislation.gov.uk/ukpga/1997/40/contents

Data Protection Act 1998
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 200
http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Appendix A


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 place?
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
YES
NO
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 7634
If it involves a member of staff contact the LADO on 01245 436744
Go to next 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


Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an e-safety incident where no illegal activity has taken place
The Headteacher/e-Safety Co-ordinator should:
Record the incident in the e-safety log
Keep any evidence
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 01245 436744
Review evidence and determine whether the incident was accidental or deliberate
Decide upon the appropriate course of action
Follow school disciplinary procedures (if deliberate) and contact Schools HR on 01245 436120 or your schools Link Officer
Did the incident involve a member of staff?
YES
NO
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
Was the Child the victim or perpetrator?
Pupil as Victim
Pupil as Instigator
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 0845 603 7634
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

Appendix B

Acceptable Use Agreement: Pupils

Moulsham Junior e-safety charter

- I will only use my Purple Mash e-mail for school purposes.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my Computing passwords.
- I will only open, delete or change my own files.
- I will make sure that all Computing contact with other children and adults is 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 an adult immediately.
- I will not give out my own details such as my name, phone number or home address to anyone over the internet.
- I will not arrange to meet anyone over the internet.
- I will be responsible for my behaviour when using Computing because I know that these rules are to keep me safe.
- I know that my use of Computing can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-safety.
- If I am unhappy with anything on the internet I will report it to an adult as soon as possible.

Appendix C

Moulsham Junior School

Sharing, Supporting, Striving, Succeeding

Princes Road, Chelmsford, Essex CM2 9DG

Telephone: 01245 352098

Email: admin@moulsham-jun.essex.sch.uk
Website: www.moulsham-jun.essex.sch.uk
Follow us on Twitter: @Moulshamjunior

Headteacher: Mrs M Staley B.A. Q.T.S. N.P.Q.H.
Deputy Headteacher: Mrs G Moores B.Sc. P.G.C.E.

Dear Parent/ Carer,

Computing 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 Computing.

Please read and discuss these E-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 Computing Co-ordinator or the Deputy Headteacher.

This Acceptable Use Agreement is a summary of our E-Safety Policy which is available in full via our publications scheme on our website.

✂ .....

Parent/ carer signature
We have discussed this and …….....(child name) agrees to follow the E-Safety rules and to support the safe use of Computing at Moulsham Junior School.

Parent/ Carer Signature ……

Class …… Date ……

Appendix D

Moulsham Junior School

Sharing, Supporting, Striving, Succeeding

Moulsham Junior School

Child's Name:_____ **Date:**_____

Please complete this form and return it to the School Office as soon as possible. The information you supply on this form will be held on our computer system. If you do not wish any of the information to be held electronically, please indicate this on the form where appropriate. If you have any queries please do not hesitate to contact us. Thank you.

Local Trips

From time to time, as part of their school topic work children need to visit places of local interest such as Oaklands Park, the library, Chelmsford Cathedral and Tesco's. These trips are always within school hours and are fully supervised. You will be informed of the detailed plans of these visits prior to them taking place.

I give permission for my child to participate in any local trips organised by the school for the duration of their time at Moulsham Junior School.

Signed:_____ (Parent / Guardian)

Medical

Does your child suffer from any allergies / medical conditions, including asthma.
Yes / No

If yes, please give details of all conditions and information about any medication:

_____

_____

_____

Please continue on a separate sheet if necessary. Named inhalers must be carried by your child at all times if required.

Website

Our website, www.moulsham-jun.essex.sch.uk is created using software linked to/endorsed by Essex Local Authority (L.A). We would like to publish children's work and class activity photographs online. Please indicate below whether you would like your child's unnamed photograph (these will be discrete) to be included.

I give permission for my child's unnamed photograph to be included on the school website **Yes / No**

Signed…… Parent/Guardian
Name of Parent / Guardian (please print)……..

Photography/Video

I give permission for my child to be photographed / videoed during school performances and similar events such as sports day, carol services, productions, visits to other schools and school trips, for the duration of their time at Moulsham Junior School.

Yes / No

Signed……parent/guardian

I give permission for my child to be photographed/filmed for articles that may appear in the press or TV programmes. **Yes / No**

Internet Use

As part of your child's curriculum and the development of Computing skills, providing
access to the internet is of vital importance. Our school internet provider operates a filtering system that restricts access to inappropriate materials. Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of the children to access inappropriate materials through the internet, the school will not be liable for any damages arising from your child's use of internet facilities.

I give permission for my child to have access to the internet **Yes / No**

Signed ……parent/guardian

Name of Parent / Guardian (please print)……

We have devised a set of rules for responsible internet use which we will regularly talk through with your child as part of our e-safety curriculum. We request that you read through the following rules with your child, and then ask them to sign below.

We use the school computers and internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

- I will ask permission before entering any Web site, unless my teacher has already approved that site
- I will not look at or delete other people's file
- I will not bring removable storage devices into school without permission
- I will only e-mail people I know, or my teacher has approved
- The messages I send will be polite and sensible
- When sending e-mail, I will not give my home address or phone number, or arrange to meet someone
- I will ask permission before opening an e-mail or an e-mail attachment sent by someone I do not know
- I will not use Internet chat
- If I see anything I am unhappy with or I receive message I do not like, I will tell a teacher immediately
- I know that the school may check my computer files and may monitor the Internet sites I visit
- I understand that if I deliberately break the rules, I could be stopped from using the Internet or computers.

I have read and understood the rules for responsible internet use. I will use the computer system and internet in a responsible way and obey these rules at all times.

Signed by pupil……

I have discussed the above with my child.

Signed by Parent / Guardian……..

Appendix E

Acceptable Use Agreement: Staff, Governors and Visitors

Staff Computing Acceptable Use Agreement

The agreement below is an overview of the acceptable use, by staff, of Computing at Moulsham Junior School. We have an acceptable use agreement to ensure staff are aware of their responsibilities when using Computing. The e-safety and acceptable use policy explains the provision for e-safety throughout the school.

How staff use school Computing
School Computing equipment, including the internet, should be used for school related purposes. Personal use is accepted on the provision usage is in accordance with this agreement, the e-safety policy and deemed reasonable by the deputy or head teacher.

When Computing equipment is to be used, which is not at a fixed location, it is to be booked out using the equipment booking register found in the Computing suite.

If laptops, iPads or other mobile devices are to be taken off site they must be signed out, via the Computing technician, this is so we know exactly which piece of equipment is where at any time. County guidance is that laptops and other mobile devices are not to be left in cars unattended.

Child safety
It is our responsibility to educate and support our pupils to use electronic devices and the internet safely. We also have a responsibility to report to the e-safety officer (Computing co-ordinator)
any e-safety issues which will be followed up and acted upon.

Social Networking
Social networking sites must not be accessed in school hours, by staff using the schools facilities, including the internet, for personal use. Social networking can be accessed for educational purposes where permission is granted by the deputy or head teacher. e.g. Twitter account to report school sports or snow days, class blog to share children's work. If social networking is to be used age restrictions are to be upheld.

School related business is not to be discussed using social networking; this includes 'private' or 'direct messaging' as is stated in the Code of Conduct. As a member of the school community we have a responsibility for upholding the Code of Conduct, which states use of social networking must not adversely affect the reputation of the school or bring the school into disrepute.

Befriending of pupils and ex-pupils from our school who are (with the exception of family members) under the age of 18 is not advisable. Befriending of parents is acceptable but discussions of school related business or posting any comments or actions that could adversely affect the school is not acceptable.

e-mail
All e-mails involving school business are to be sent and received using the allocated school e-mail address. All e-mails from this account are to include a school disclaimer signature at the bottom of the page which will be attached as a template for all e-mails. Only the office staff, deputy or head teacher can e-mail parents directly regarding school related business. We can e-mail children from our school but only from and to a school e-mail account.

Audio, Video and Photography
Audio, video and photographic files remain the property of the school at all times. These are to be stored on the school server or mobile devices (iPad, cameras). These types of files are to be used for school related business; they can be taken and used off site but you are responsible for safe guarding the files and minimising risks.

Only school equipment is to be used by staff for recording audio, video or photographic files. Personal equipment is not to be used under any circumstances for recording these files – this is to safeguard you. You are able to use personal equipment to edit, manipulate and produce resources for these file types but you are responsible for safe guarding the files and minimising risks.

File sharing
File sharing, including the use of removable devices (memory sticks) and cloud based technologies (DropBox), is the responsibility of the user to safeguard the information being used and minimise risks. Encrypted memory sticks can be supplied upon request.

Remote access
You can remotely access the school network from any location but it is the responsibility of the user to safeguard the information being used and minimise risks. You must ensure that the device in which you are accessing the school network from is up to date with its latest anti-virus and malware software.

Personal Devices
When at school, whilst children are on site (8:45-3:15), personal devices such as mobile phones, tablet computers and laptops should not be used for personal use other than in staff areas e.g. staffroom, PPA room, office areas. Personal tablets and laptops can be used for educational purposes but you must ensure that they are free from virus and malware if they are to be connected to the schools network. Please refer to the above section regarding audio, video and photography.

If you have any queries, are unsure of anything or do not have a definitive answer for, please seek advice from Computing co-ordinator or the deputy head teacher before proceeding.

Any breaches of this agreement, could lead to action under the Disciplinary procedure, including dismissal in serious cases.

I confirm that I have read and understood the above.

Received on: ……

Name (please print) ……