Moulsham Junior School

E-Safety Policy

(Encompassing Internet access and digital safeguarding policy)

Reviewed with Staff: December 2019

Ratified by Governors: Spring 2020

Next review: Spring 2024

Moulsham Junior School

E-safety

and

Data Security

Guidance Policies for Computing Acceptable Use

CONTENTS

Introduction

This Policy sets out Moulsham Junior School's aims, principles and strategies for the delivery of E-Safety through the Computing Curriculum. Computing in the 21st Century is an essential resource to support learning and teaching it is our duty to ensure pupils are developed with the skills to access life-long learning and employment as well as to develop a secure understanding of safe and responsible use. Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning.

This policy also outlines our purpose in providing access to the Internet and how Moulsham Juniors seeks to avoid the potential problems that unrestricted access could give rise to. The purpose of Internet access in school is to raise educational standards, inform parents of work undertaken, support the professional work of staff and to enhance the schools' management information and business administration systems.

What is ICT?

ICT comprises a set of concepts and skills for using and communicating information.

Information and Communication Technology includes, but is not limited to, the use of:

- Audio and video recorders,
- Digital still and movie cameras, scanners
- Electronic musical instruments and sound mixing equipment Computers, laptops, tablet devices,
- Programmable toys and control kits e.g. Beebots, Roamer
- Assistive technology
- Voice-operated equipment
- The internet, including social networking and blogging (Purple Mash)
- Interactive whiteboards and similar interactive presentation technologies
- Software
- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Blogs and Wikis

ICT helps students take greater responsibility for their own learning, plan and organise their ideas, and produce and present work of a high standard. It also enhances creativity. 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. A whole school approach to e-safety helps to ensure staff, governors and parents know how to help pupils to behave responsibly online.

Government guidance highlights the importance of safeguarding pupils from harmful and inappropriate online material (Department for Education, 2019a). This includes material accessed through devices such as computers, laptops, tablets and mobile phones, as well as platforms such as social media and online games. In England, the Department for Education (DfE) has published non-statutory guidance on teaching online safety in school (PDF). (DfE, 2019b)

Aims

Through the Computing Curriculum Moulsham Junior School aims to:

- make sure staff and volunteers are confident in teaching online safety, identifying and responding to concerns through having the most up to date information.
- teach children and young people the skills to stay safe online
- share helpful advice and resources with parents and carers
- develop robust e-safety policies and procedures, IT infrastructure and support
- regularly review and improve our e-safety provision.

E-safety in 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 lesson.

• 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, modelling 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.

Moulsham Junior School's aims of Internet use.

• To access world-wide educational resources.

• Participate in Government and National initiatives.

• To enable the professional development of staff by providing access to educational materials and good curriculum practice.

• To allow the exchange of curriculum and administration data with LA and DFES.

• To share work with other schools and parents.

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).

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.

Monitoring

E-safety Skills Development for Staff

• Our staff receive regular information and training on e-safety issues through staff meetings.

• 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.

• All staff are expected to incorporate e-safety activities and awareness within their curriculum areas.

How the use of the Internet at Moulsham Junior School will be managed safely

The Internet has a number of associated dangers and these must be managed. The digital world moves very quickly and staff are constantly risk assessing any new programmes, websites or procedures to ensure the safety of pupils is maintained.

• E-safety is a compulsory part of the Computing Curriculum. Pupils will be taught appropriately to their age, to use the Internet responsibly in order to reduce the risk to themselves and others.

• Any issues regarding Cyberbullying/ E safety will be reported to SLT/ ICT Co-ordinator. A record will be kept of such incidents and form part of our safeguarding recordings.

• Pupils will be encouraged to use 'Safe Search' to access learning materials.

• Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils. Staff will be particularly vigilant regarding pop ups and advertising commercials.

• SMART thinking posters will be displayed prominently in ICT areas.

• Our Internet access is purchased from Essex County Council which provides a "Firewall" filtering system intended to prevent access to inappropriate material for children.

• Use of digital storage devices will be reviewed on a regular basis.

• The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.

• 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

• Staff and pupils must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.

• Staff must not reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog

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

E-mails

Sending e-mails

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'. Pupil's e-mails can be accessed and monitored through Purple Mash as an additional layer of protection.

Managing e-mail

• Moulsham Junior 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

Monitoring of equipment.

Authorised Computing staff may inspect any Computing equipment owned or leased by the School at any time without prior notice. School staff will always ask for their identification badge and contact their department to clarify their role and the 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. See Appendix A- Flow Chart for dealing with both illegal and non-illegal incidents.

Misuse and Infringements

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.'

Computer Viruses

• All files downloaded from the Internet, received via e-mail or on removable media (e.g. memory sticks, CD) must be checked for any viruses using school provided anti-virus software before using them

• If it is suspected that 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.

The school follows the Department for Education guidelines.

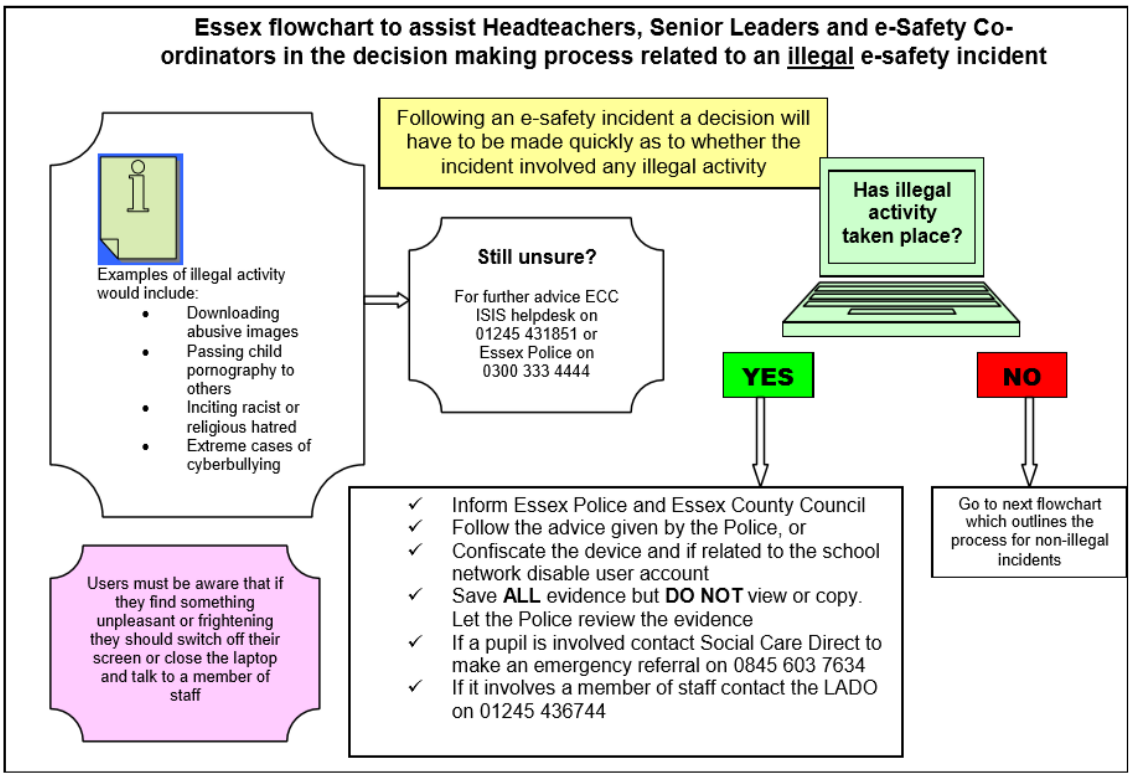
http://www.education.gov.uk/schools/pupilsupport/pastoralcare/b00198456/principles-of-e-safety

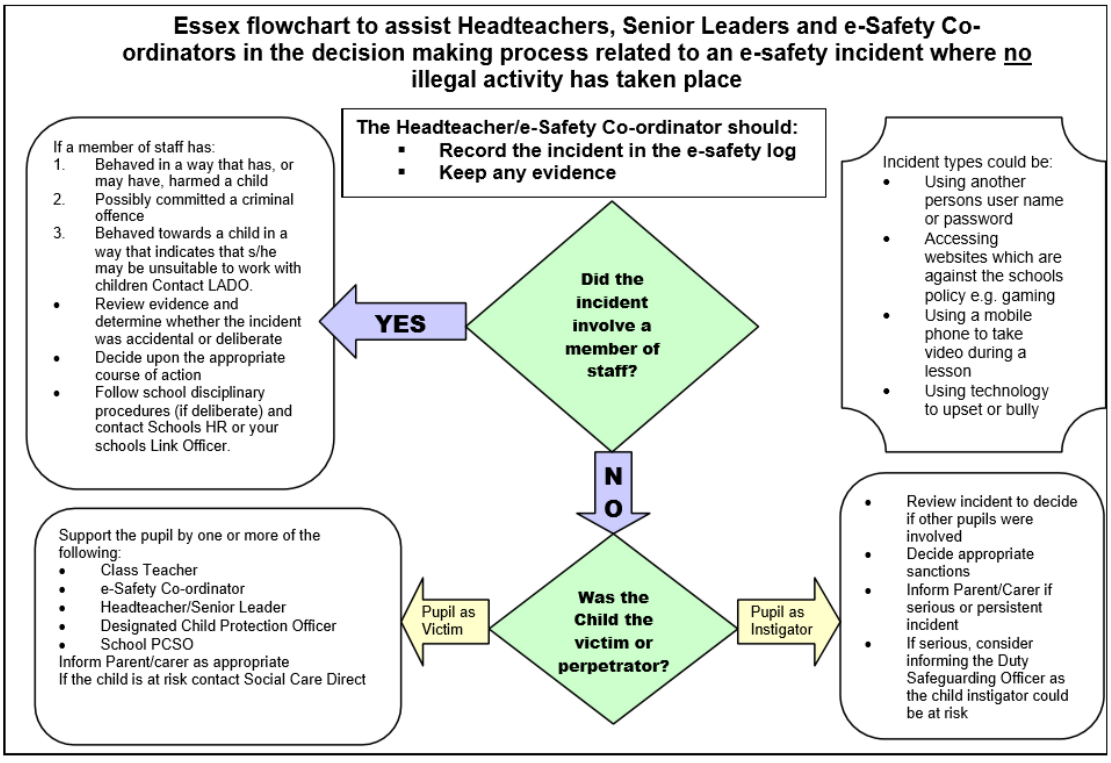
Security

- 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
- 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 not remove portable devices from the school premises.

- 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 mopiers (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:

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.
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 or your schools Link Officer.
YES
Did the incident involve a member of staff?
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
NO
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
Pupil as Victim
Was the Child the victim or perpetrator?
Pupil as Instigator
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

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, iPad 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 coordinator) 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 school's 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 (Drop Box), 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 school's 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) ……