Amended March 2015

Amended November 2015

Amended April 2017

Jotmans Hall Primary School

E Safety & AUP Policy

Approved by the Finance & Premises Committee on …………………………………….

Accepted/Ratified by Full Governing Body on …………………………………….

Amended March 2015

Amended November 2015

Amended April 2017

Jotmans Hall Primary School
E-Safety and ICT Acceptable Use Policy for Pupils and Staff

1. Introduction

- Our E-Safety and ICT Acceptable use Policy (AUP) has been written by the School, taking into consideration Local Authority and Government guidance. It has been agreed by the Senior Leadership Team and approved by Governors. It will be reviewed annually.
- Use of the school's ICT equipment by any members of the school community must be in accordance with this policy. Any use which infringes this policy will be treated very seriously by the school Governing Body.

2. Why the Internet and Digital Communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

3. Internet use will enhance and extend learning

- The school Internet access will be designed expressly for pupil use and will include appropriate filtering.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

4. Pupils will be taught how to evaluate Internet content

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

5. Information system security

- School ICT system security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

6. Management of Pupils' School E-Mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.

7. Management of School Website Content

- The contact details given online will be the school address, school e-mail and telephone number. Staff or pupil personal contact information will not be published,
- Photographs that include pupils will be selected carefully and will not enable individual students to be clearly identified.
- Pupils' full names will not be used anywhere on the school website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

8. Pupil's' Use of Social networking, chat rooms and personal publishing

- The school will block access to social networking sites, and consider how to educate students in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will not be allowed access to public or unregulated chat rooms.
- Pupils should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.

9. Managing filtering

- Access to the Internet is provided to the School by Essex Local Authority. The School will work in partnership with Essex Local Authority ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator or a member of the SLT.

10. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is allowed.
- Mobile phones will not be used by pupils during lessons or formal school time – they will be handed in to the School office during the school day.

11. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

12. Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access (a copy of the letter is included in the appendix).
- Parents will be asked to sign and return a consent form.

13. Assessing Risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for children. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Essex LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

14. Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.

15. Informing Pupils about the E-Safety and Acceptable Use Policy

- e-Safety rules will be posted in all rooms where computers are used.
- Pupils will be informed that network and Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.

16. Staff and the E-Safety and Acceptable Use Policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.
- Staff will maintain a professional attitude when using Social Networking Sites out of school hours and carefully consider who they correspond with and the content of any communication. The School strongly discourages the use of such sites to correspond with parents or pupils, to protect all parties' privacy.

17. Enlisting Parental Support.

- Parents' attention will be drawn to the School Internet Policy in newsletters, and on the school Web site.

Appendices:

1) **E-Safety Rules**
2) **Letter to parents on Responsible Internet Use**
3) **Consent Form**
4) **Staff Code of Conduct for ICT**

Amended March 2015

Amended November 2015

Amended April 2017

Appendix 1 – E-Safety Rules

E-Safety Rules

These e-Safety Rules help to protect pupils and the School by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.

- Copyright and intellectual property rights must be respected.

- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The School ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Letter to parents on Responsible Internet Use

Appendix 2 – Letter to Parents

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, Jotmans Hall Primary School provides supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please read the attached E-Safety Rules and sign and return the consent form so that your child may use the Internet at school. If you wish to see a copy of the school's 'E-Safety and Acceptable Use Policy' this is available on the school website in the Parents section.

Although there are concerns about pupils potentially having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school 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 children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

Yours sincerely

Nicki Kadwill
Headteacher

Jotmans Hall Primary School

E-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Student: ____________________________________ ***Class :*** _________

Pupil's Agreement

I have read and I understand the school e-Safety Rules. I will use the computer network, mobile phones, Internet access and other new technologies in a responsible way and follow these rules at all times. I know that network and Internet access may be monitored.

Signed: ____________________________________ ***Date:*** ______________

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: ____ ***Date:*** ______________

Please print name: ____

Amended March 2015

Amended November 2015

Amended April 2017

Staff Code of Conduct for ICT

Appendix 4 – Staff code

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's E-Safety and Internet Acceptable Use Policy for further information and clarification.

- 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 appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras; email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher. This means that I will not allow my family or others to use my School laptop etc.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Designated Child Protection Officer or her Deputy.
- Images (both photo and video images) of pupils will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent/carer.
- I will consider the security of my laptop as a priority by ensuring that the laptop is safely stored, charging, in the storage trolley at the end of the day or taken straight home at the end of the school day. I will NOT leave it in my car or on display in my classroom unattended. I understand that the School Insurance Policy does not cover equipment left in an unattended vehicle or left out on display either at home or at School. I understand that I may be asked to pay for a replacement if these rules are not adhered to.
- I will switch off all ICT equipment at the end of the day and comply with energy saving solutions as appropriate.

- I will report any ICT faults on the '"ICT Faults" spreadsheet on the computer desktop or to the appropriate manager as soon as possible.

- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

- I understand that I have a responsibility under the School's "Whistle Blowing" Policy to report any known misuses of technology including unacceptable behaviour by members of staff, parents or pupils.

- I will not browse, download or upload material that could be considered offensive or illegal.

- I will not send to pupils or colleagues material that could be considered offensive or illegal.

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role and will not bring the School into disrepute.

- I will maintain a professional attitude when using Social Networking Sites out of school hours and carefully consider who I correspond with and the content of any communication. I understand that the School strongly discourages the use of such sites to correspond with parents or pupils, to protect all parties' privacy.

- If an inappropriate site or image is accessed during a lesson I will play down the situation. I will report the incident immediately to the Headteacher or member of the SLT and ensure that the incident is recorded in the Offensive Comments file.

- It is accepted that Staff will need to use USB memory sticks to transfer data between home and School and vice-versa. You must ensure that your home computer system has up to date anti-virus software installed and running.

- If pupil or staff data is taken off site the USB memory stick must be encrypted/password protected or the individual file must be password-protected.

- It is suggested that a software program "Autorun.eater" is loaded onto any computer/laptop used which will automatically check a USB memory stick when it is plugged

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Print name: ____

Signed: ______________________________________ ***Date:*** _______________

E-Safety Tips for Staff

Appendix 5 – Staff tips

1 If an inappropriate site or image is accessed during a lesson, play down the situation.

2 Always report the incident immediately to the Headteacher or member of the SLT. Ensure that the incident is recorded in the Offensive Comments file.

3 Don't assume that it is the pupil's fault, once blamed a pupil may never confide again.

4 Be vigilant when asking pupils to search for images. Always test an image search before demonstrating in class.

5 Encourage pupils to report inappropriate use of mobile phones, email or internet by either bullies or adults.

6 Regularly remind pupils of key e-safety messages such as "never give out personal details online".

7 Teach Internet Safety as an integral part of the curriculum, including the use of chat rooms and social networking sites.

8 Liaise with parents and carers to ensure the e-safety of pupils out of School.

9 Ensure that any pupil or staff data taken off site on a USB memory stick is encrypted/password protected or the individual file is password-protected.

10 Staff can access further information about e-safety from BECTA at :-
Search Becta's ICT Advice services for teachers

It is very important that this Policy is adhered to – penalties for unacceptable use may result in:-

- Temporary suspension of ICT services
- Disciplinary action or
- Legal intervention

The penalty will depend on the seriousness of the incident.

Amended March 2015

Amended November 2015

Amended April 2017

Staff Laptop Loan agreement

Appendix 6 – Laptop

Part of Jotmans Hall Primary School's Improvement Plan is to provide laptop computers to staff to assist in the delivery of the National Curriculum and with teachers' planning.

A laptop computer is to be **loaned** to you while you remain employed at this school. While the laptop is in your care the following items should be noted:

1. The Laptop remains the property of Jotmans Hall Primary School and is only for the use of the member of staff it is issued to – not for family members or other people.

2. Pupils must not be given access to the laptop for any reason.

3. The laptop is insured for use in School and should be stored, charging, in the storage trolley at the end of the day and not left out on display unattended. The laptop is also insured for you to take it home and in transit providing that you DO NOT leave it in your car unattended or leave it out on display at home unattended.

4. Any charges incurred by staff accessing the Internet from home are not chargeable to the school. I.e. it is your responsibility to pay for broadband/dial-up connections at home.

5. Any additional work-related software you add must be fully licensed. Proof of licensing may be asked for.

6. If the laptop requires restoring due to games or non work related software being installed, security will be increased to prevent further software installations.

7. It is your responsibility to backup any work stored locally on the laptop, work copied to the network will automatically be backed up for you.

8. If the IT Technicians or SLT request to see the laptop (for maintenance/updates etc.), you must return the laptop promptly.

9. At the end of your employment at the school, it is your responsibility to return the computer and all ancillaries to the IT Technicians / SLT prior to departing.

Laptop Make:	**Model:**	**Serial Number:**
Name:		

I have received in good order the following: (tick box as appropriate)

Laptop □

Charger □

I have read and understand the terms and conditions set out above for the loan of a school laptop.

Signature: ***Date:***

Amended March 2015

Amended November 2015

Amended April 2017

Email Policy

Appendix 7- e-mail policy

Introduction

The purpose of this policy is to ensure the proper use of the School's email system and make users aware of what Jotmans Hall Primary School deems as acceptable and unacceptable use of its email system. The School reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

Legal risks

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of using e-mail.

If any employee:

- Sends emails with any libellous, defamatory, offensive, racist or obscene remarks, the employee and the School can be held liable.
- Forwards emails with any libellous, defamatory, offensive, racist or obscene remarks, the employee and the School can be held liable.
- Unlawfully forwards confidential information, the employee and the School can be held liable.
- Unlawfully forwards or copies messages without permission, the employee and The School can be held liable for copyright infringement.
- Sends an attachment that contains a virus, the employee and The School can be held liable.

Legal requirements

The following rules are required by law and are to be strictly adhered to:

- It is strictly prohibited to send or forward emails containing libellous, defamatory, offensive, racist or obscene remarks. If e-mails of this nature are received, a Member of SLT MUST be notified
- Under normal circumstances an e-mail message or attachment should not be forwarded or copied without acquiring permission from the sender or originator first, although professional judgment may need to be applied in some cases – e.g. in forwarding data received from the LA, a parent or colleague where it is clear that this is required
- Unsolicited email messages should not be sent.
- Email messages must not be forged or forgery attempted.
- Email messages must not be sent using another person's email account.
- No person should disguise or attempt to disguise their identity when sending mail.

Best practices

The School considers email as an important means of communication and recognises the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Therefore The School wishes users to adhere to the following guidelines:

Amended March 2015

Amended November 2015

Amended April 2017

Guidance for the writing of emails:

- Write well-structured emails and use short, descriptive subjects.
- The School's email style is informal. This means that sentences can be short and to the point. It is acceptable to start e-mails with 'Hi', or 'Dear', and the name of the person. The use of Internet abbreviations and characters such as "smiley's" however, is not encouraged.
- Always use a spell checker before sending any emails.
- Do not send unnecessary attachments, save them on the shared drives and direct people to their location.
- Do not write emails in capitals.
- Do not unnecessarily use cc: fields unless the cc: recipient is aware of what action they are to take, if no action is required then mark for "information only".
- When forwarding an email message, state clearly what action the recipient should take.
- Ensure that emails marked as important really are important.

Maintenance:

It is good practice to delete email messages that you do not need a copy of, remembering to empty the deleted items folder at least once a week. You have a set amount of storage space (default = 200Mb). Once this is full you will not be able to receive new messages.

Personal Use

Personal use is use that is not directly connected with an employee's job function. Although The School's email system is meant for business use, the School allows the reasonable use of email for personal use if certain guidelines are adhered to:

- Personal use of email should not interfere with work.
- Personal emails must also adhere to the guidelines in this policy.
- The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.
- Mass mailings are prohibited.

All messages distributed via the School's email system, even personal emails, are the School's property.

Confidential information

Avoid sending confidential information by e-mail. If this is done the information should be secured by including it in a Microsoft Word or Excel file and protecting it with a password which can be provided to the recipient by other means.

Amended March 2015

Amended November 2015

Amended April 2017

Relationship to other Policies

When using email for business or private communication purposes, either internal or external, staff must pay due regard to the School's expected standards of conduct as expressed and required through its published policies and procedures. Policies particularly relevant include harassment and bullying, equality and diversity and whistle-blowing.

System Monitoring

You must have no expectation of privacy in anything you create, store, send or receive on the School's computer system. Your emails can be monitored without prior notification if the School deems this necessary. If there is evidence that you are not adhering to the guidelines set out in this policy, then The School reserves the right to take disciplinary action, including termination and/or legal action.

Email accounts

All email accounts maintained on our email systems are the property of the School. Passwords should be considered very confidential and if you believe it is no longer secure please inform the Live@EDU Helpdesk, Becky Chapman bfry@jotmanshall.essex.sch.uk or Caroline Fox/Emma Nunn admin@jotmanshall.essex.sch.uk immediately.

Questions

Any questions or comments about this Email Policy should be directed to the Headteacher, email: head@jotmanshall.essex.sch.uk All employees of The School are expected comply with this policy.

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of e-mail. If any user disregards the rules set out in this Email Policy, the user will be fully liable and the School will disassociate itself from the user as far as legally possible.