THE BETTY LAYWARD PRIMARY SCHOOL
Internet Security Policy (AUP)

Revised January 2016

The purpose of internet access is to raise educational standards and enhance the educational experience of our pupils, to support the professional work of staff and to enhance the school's management, communication and business administration systems.

The statutory curriculum currently requires pupils to learn how to locate, retrieve, exchange and present information using ICT. Web-based resources skills are vital to life-long learning and employment; ICT is an essential life skill. In the Betty Layward curriculum, teachers plan to integrate the use of ICT for the benefit of our pupils.

Most technologies present risks as well as benefits. At Betty Layward we adopt the strategies for the safe and responsible use of the internet in accordance with The Learning Trust IT Services Guidelines. In line with school policies that protect pupils from other dangers, we endeavour to provide our pupils with as safe an internet environment as possible and teach them to be aware of and respond responsibly to any risks. Pupils, teaching and support staff and parents/carers are all asked to play their part in assisting pupil to use the internet responsibly and safely.

Betty Layward Core Principles of Internet Safety

Effective use of the internet will be essential for all pupils in later life. However, unmediated internet access brings with it the possibility of placing pupils in unwelcome, inappropriate and potentially dangerous situations.

Our Internet Safety Policy is built on the following five core principles:

Guided educational use
Curriculum use of the internet is planned by teachers, and focused on particular tasks within a supervised and managed environment. Pupils' internet use is supervised at all times. We do not believe that pupils' browsing the web in an undirected way is educationally productive. At KS1 pupils

either watch teachers accessing the internet to retrieve information or use specified sites themselves which have been fully checked. At KS2 pupils are learning to find information for themselves, to use appropriate key words and to progress on from child-friendly search engines, in a supervised environment. Pupils will be given clear objectives for internet use at all times.

Risk assessment
All pupils are made aware of the principles of e-safety through specific teaching and all pupils sign a computer use Code of Conduct which they are expected to adhere to. Each academic year begins with a series of e-safety lessons in years 2-6, whilst each Computing lesson includes content regarding internet safety for that particular lesson. Issues are also returned to in PHSE lessons during the year and at other times eg Anti-Bullying Week, Safer Internet Day, and our end of Spring Term e-safety workshops for pupils, parents and staff. Pupils are informed that checks can be made on files held on our network. Pupils receive guidance on what to do if they come across inappropriate material. Specific KS2 assemblies are conducted each term regarding specific aspects of internet safety, such as: the safe use of social media, online communication and actions to be taken when issues occur.

Responsibility
Internet safety depends on staff, schools, parent/carers and pupils themselves taking responsibility for the use of the internet and other communication devices such as mobile phones. The balance between education, communication and entertainment is discussed with pupils encouraging them to take an informed responsible approach.

Regulation
The use of our expensive computer systems requires some straightforward rules and guidance to be in place for everyone's benefit. Misuse, or damage, is unacceptable and computer access will be denied if necessary. Chat rooms are not allowed to be accessed by pupils in school. Mobile phones are only to be brought to school by students in year 6 and they are stored securely without use during school hours. Internet rules, which are clearly understood by pupils through discussion, are on display in classrooms and the ICT suite.

Appropriate strategies
This document describes strategies to help ensure responsible and safe use. We base these on supervising access, developing responsibility and on guiding pupils towards educational activities. Staff, parents/carers and the pupils themselves are all expected to show a well informed and vigilant approach.

Betty Layward School Internet Safety Policy

The Internet Safety Policy is part of the ICT Policy and School Improvement Plan and relates to other policies including the Learning Trust IT Services Guidelines for Safe Use of the Internet in Schools.

The following activities are strictly prohibited:

- Use of the internet to harass, offend or bully any other person.
- Use of the internet for any inappropriate or illegal purpose.
- Use of the internet for transmission or reception of threatening or obscene material.
- Use of the internet for transmission or reception of material from any criminal organisation.
- Use of the internet for the transmission or reception of viruses or unlicensed software.
- Use of the internet for any personal, commercial purpose or profit.
- The 'use of the internet' also implies the use of personal devices or other internet capable mobile communication devices in school.

Responsibility

The Headteacher is designated as responsible for student safety and security policies related to the internet and electronic communications.

The Headteacher, along with the Computing Coordinator and Network Administrator ensure that policies are implemented and regular monitoring takes place. All staff (and visitors using the internet) are made aware of school policies. All users are encouraged to use computers and the internet responsibly and for the educational purpose intended to understand the consequences which their actions could have on themselves and others.

Acceptable Use

Pupils, staff and any other adults with internet access must sign an Acceptable Use Policy Agreement.

Such an agreement makes everyone aware of their responsibilities when using the internet.

Pupils

- Parents are informed through the internet safety policy, and by letter, that pupils will be provided with supervised internet access.
- All school users, staff and pupils, are required to sign an Acceptable Use/Code of Conduct agreement from Y2 upwards, appropriate to their key stage.
- The school keeps a record of any pupils who are denied internet access and the child's class teacher and parents are informed.

Betty Layward School will take all reasonable precautions to ensure that users access only appropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the Learning Trust IT Services can accept liability for the material accessed or consequences of internet access.

- All internet access is supervised.
- Rules for internet access are posted in all rooms where computer are used.
- Pupils are informed that internet use will be monitored.
- Instruction is given in responsible and safe internet use covering both school and home use.
- If pupils discover unsuitable sites, the monitor should be turned off, or laptop closed, the URL (address) and content should be reported to the teacher, Computing Coordinator and the Network Administrator.
- Appropriate Child Protection Policy must be followed in instances where unacceptable use has raised child protection issues.
- Teachers should follow the school's 'Prevent Duty' policy if any issues regarding radicalisation of students arise. The Computing Co-ordinator will communicate with the Headteacher regarding any potential radicalisation issues for appropriate action to be taken on a case by case basis.

Staff

It is important that our teachers and support staff are confident to use the internet in their work. They also need to use the internet with professional responsibility.

- Staff are required to use their school user names and password-protected log ons when accessing the internet and to log off when they have finished.

- Staff are made aware that internet traffic can be monitored and traced to the individual user. School internet access is for matters pertaining to school work only, other than brief checking of email messages or websites during break times. Staff are not allowed to download, upload or print personal information or pictures. Disciplinary action may be taken if the internet is used inappropriately eg for accessing pornographic, racist or offensive material or for personal financial gain, gambling, political purposes (including terrorism or radicalisation content) or advertising.
- All staff are required to sign and adhere to the school Computer Acceptable Use Policy.

Use of email

Staff emails are recorded, can be traced back to the sender and can be legally binding. Staff must inform the designated persons if they receive offensive or threatening emails. Staff should ensure that they do not engage in private personal correspondence with pupils.

Pupils can be provided with a school email address when they reach Year 3. Our school email is private, hosted by London Grid for Learning, is subject to monitoring and can be managed.

- Pupils are taught to use email safely and responsibly.
- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive email. The designated persons will be then be informed.
- Pupils must not reveal details of themselves or others in email communication, such as address or telephone number, or arrange to meet anyone.
- Offensive messages or posts sent by pupils out of school concerning other pupils or staff, will be dealt with under the remit of the school internet safety policy.

Virus Protection

All computers used for access to the internet must have regularly updated anti-virus software installed. Any user who suspects the presence of a computer virus must alert the Computing Coordinator who will alert the Network Administrator/Technician immediately.

Copyright and authenticity

Copyright rules apply to material available over the internet. Many sites carry copyright warnings indicating how the material may be used and how to obtain permission.

Staff should

- Never assume that educational use of material is permitted, without first checking with the author or publisher.
- Be aware that work published on websites may be open to unauthorised use.
- Be aware that publishing other people's material without their permission is a breach of copyright. This also applies to images.

According to their age, **pupils** will come to learn and appreciate:

- That information gained from websites should be used selectively.
- That thought should be given to its relevance to the task.
- Respect for copyright and intellectual property rights is important.
- That there are correct ways to use published material.

Our school website and social media pages

Our **website** and 'Instagram' account is intended to provide information to parents/carers and others, and show selected information about our school and activities.

- Parents/carers will be given the opportunity to refuse the inclusion of photos of their children on the website/Instagram account.
- Students do not have editing rights to either the school website or social media pages. The Headteacher, Senior Leadership Team, Computing Co-ordinator and Administrative team are the only staff with any editing or posting rights. This is at the discretion of the Headteacher and can at any point be deemed necessary to make changes to posts as required
- All staff have the responsibility to report any issues regarding the website, twitter page and Instagram account to the Computing Co-ordinator and the Headteacher at the earliest opportunity after an issue arises.

Chat rooms and social media

The use of chat rooms and social media pages by students is not permitted in school. Outside school, we recognise that pupils do use a variety of chat facilities and social media pages and may not be fully aware of the potential dangers. Pupils will have opportunities to learn about and discuss safe use of chat facilities and social media in e-safety and PSHE lessons, and school assemblies during e-safety and anti-bullying weeks.

Mobile phones

Mobile phones are only permitted to be brought to school by children in Year 6 who walk home alone. Phones must be handed in to the pupil's class teacher in the morning and handed back at the end of the day. They are not to be used at all during school time. The sending of abusive or inappropriate text messages or photos would be dealt with under the school anti-bullying procedures and internet sanctions would be put in place.

Staff may only use their own mobile phones during out-of-class personal break times, not during teaching time with pupils or whilst on playground or lunch duty. It is not acceptable for staff to use their phones to take photos of pupils.

Security of the school networked system

This responsibility falls within the remit of the School IT Technicians and the Learning Trust, which maintains and reviews the security and functionality of the school networked systems. This includes:

- Virus protection which is installed and updated regularly
- Being available to monitor files held on the school's network when necessary
- Maintaining the provision of filtered access
- Installation of hardware and software on the school networks.

Jason Stuart, Computing Coordinator January 2016
jstuart@bettylayward.hackney.sch.uk

Betty Layward Primary School

STUDENT RULES FOR SAFE INTERNET USE

- I will always log on with my own name and password.
- I will only use the computer in the way my teacher has told me to.
- I will only search the Internet for the topics we are learning about.
- I will tell my teacher if I see anything on the Internet which makes me feel uncomfortable. I will switch off the monitor.
- I will never give anyone's photograph, address or phone number over the Internet, including my own.
- I will only send polite and friendly emails. I will tell my teacher if someone sends me a nasty message.

Name:_____

Signature:_____

Date:_____Class:_____

Appendix 2 – Staff Acceptable Use Policy

THE BETTY LAYWARD PRIMARY SCHOOL	**Name of School**	**Betty Layward Primary School**
	AUP review Date	**January 2016**
	Date of next Review	**January 2017**
	Who reviewed this AUP?	**Jason Stuart, Computing Coordinator**

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. **email, Internet, network resources, software, equipment and systems.**

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity either inside or outside of work that may compromise my professional responsibilities.
- I will only use the approved, secure email system for any school business.
- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Headteacher.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.

- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any laptop or iPad loaned to me by the school, is provided solely to support my professional responsibilities. I am responsible for the safety and return of this item when requested by the Headteacher or Computing Co-Ordinator.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the school's named child protection officer / relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I will immediately report any student ICT issues regarding the school's 'Prevent Duty' policy (regarding radicalisation and acts of terrorism) to the Computing co-ordinator or Headteacher.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): Staff agreement form

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I wish to have an email account; be connected to the Internet and be able to use the school's ICT resources and systems.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

School .....

Authorised Signature (Head Teacher)

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)