BEECHFIELD SCHOOL

eSafety Policy
(Acceptable Use of the Internet)

Author: Lisa Roberts/Sarah Pendlebury
Date: September 2015
Approved by: School Improvement and Curriculum Committee
Date: September 2015
To be reviewed by: School Improvement and Curriculum Committee
Date: September 2017

INTRODUCTION

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

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 ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At Beechfield School we understand the responsibility to educate our pupils on eSafety 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.

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

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

EXPECTATIONS

It is expected that:

- All users of the Internet: staff, pupils, students, parents, governors, visitors and anyone else using ICT within the school or on school property, will follow the conditions in this policy.
- Any Internet user who becomes aware of access to inappropriate material shall report it immediately to the subject leader for ICT. Users should under no circumstance seek to explore or evaluate the materials further.
- The subject leader for ICT will immediately report any instances of access to inappropriate material over the Internet to the Headteacher and the relevant authorities.
- All Internet activity should be appropriate to staff professional activity or the pupils' education and should be generally supervised.
- All Internet access within the school or on school property shall be via 'the grid', which provides filtered access to the Internet. Details of this protection can be found at http://www.thegrid.org.uk/eservices/safety/index.shtml
- Access to the Internet will be made solely through an authorised account log-in and password, which shall not be made available to any other person. The school secretary will provide any visitors who require for professional purposes to access the school network, a temporary log-in using the supply laptops.
- Use of the Internet and facilities such as the electronic mail service are intended for educational purposes only and not misused for harmful or hurtful cause. Such communication should be honest, legal, decent and true.

CONDITIONS OF USE

All users must agree to the following rules.

- The school and Governing Body have an agreed set of rules for Internet use, which are designed to maximise use of the Internet as a learning resource and minimise unacceptable behaviour and access to inappropriate materials.
- All users have been made aware of the conditions of use and have agreed to abide by them.
- Parents, guardians and carers have been made aware of the conditions of use and have given their permission for their child to use the Internet in accordance with these rules by signing the Pupil Acceptable Use form (pages 10-12).
- All members of staff have agreed to the Conditions of Internet Use outlined in this document and have signed to this effect (page 13). They have been made aware of the Staff professional responsibilities advice provided by Hertfordshire County Council. (page 15). They have been made aware of the Beechfield Social Networking Staff Terms of use (page 14).
- All members of staff have been made aware of these rules and their implications regarding the possible misuse of on-line access.
- The children at Beechfield School are **taught** to use the internet sensibly. The PSHE Co-ordinator and ICT Co-ordinator raise awareness of eSafety through assemblies and age appropriate workshops. eSafety is built into the PSHE curriculum. Children are taught about the potential dangers of the internet, including email, messaging, forums, boards, social networking sites. They are also taught what to do in the event that they find something that they are not comfortable with.
- Schools and Families filter all content we receive onsite. All members of staff have accepted responsibility for explaining safe Internet use to their pupils.
- Appropriately worded copies of Conditions of Internet Use will be displayed in the ICT suite, on the laptop trolleys, in the staffroom, in the offices and on the school website.

eSAFETY

eSAFETY – ROLES AND RESPONSIBILITIES

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Sarah Pendlebury who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

eSAFETY IN THE CURRICULUM

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

- The school has a framework for teaching internet skills in Computing/ICT/ PSHE lessons.
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- eSafety Workshops are provided for KS1 and KS2 on an annual basis which are delivered by Herts for Learning eSafety advisers.
- Pupils are taught 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 Cybermentors, Childline or CEOP report abuse button.

eSAFETY SKILLS DEVELOPMENT FOR STAFF

- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see eSafety Co-ordinator)
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

MANAGING THE SCHOOL ESAFETY MESSAGES

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The eSafety policy will be introduced to the pupils at the start of each school year.
- Age appropriate eSafety displays will be found in all classrooms.
- The key eSafety advice will be promoted widely through school displays, newsletters and class activities.

eSAFETY PARENTAL INVOLVEMENT

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (eg, on school website)
- Parents are asked to sign a log if they are taking photographs or videos at school assemblies and concerts. By signing the log, should parents wish to share photos/videos on social media, parents agree to only share photographs/videos of their own children as a safeguarding measure.
- Parents/carers are expected to sign our Pupil Acceptable Use form (pages 10-12) containing the following statement
    - **We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community or bring the school name into disrepute.**
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
    - Practical training workshops eg current eSafety issues
    - School website information
    - Newsletter items

MONITORING

Authorised ICT staff may inspect any ICT 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 ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, 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 ICT; 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.

ICT authorised staff may, without prior notice, access the e-mail or voice-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 ICT 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 ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised HCC staff.

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 ICT hardware, software or services from the

offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

For pupils, reference will be made to the school's behaviour policy and Hertfordshire guidance.

INCIDENT REPORTING

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person or eSafety 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 ICT and all other policy non-compliance must be reported to the Headteacher.

SANCTIONS

If any breach of conditions is discovered the following sanctions may be enforced:
- Temporary or permanent ban on Internet use.
- Additional disciplinary action in line with the school behaviour policy.
- Parents and other external agencies may be contacted.
- eSafety Incidents will be recorded in the eSafety Incident Log.

Any breach of the conditions laid down by this policy may lead to the withdrawal of Internet access rights and could lead to disciplinary action and possible criminal prosecution. In the case of employees breach of conditions may constitute a breach of conditions of service and could lead to dismissal on the grounds of misconduct.

eSAFETY INCIDENT LOG

Details of all eSafety incidents are recorded by the eSafety Coordinator. The incident log (see page 17) is monitored termly by the Headteacher. Any incidents involving Cyberbullying may also need to be recorded elsewhere.

eSAFETY MISUSE AND INFRINGEMENTS

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the Hertfordshire Flowcharts for Managing an eSafety Incident should be followed (pages 18-21).

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see pages 18-21).

MEDIA PUBLICATIONS

Named images of pupils (e.g. photographs, videos, web broadcasting, TV presentations, web pages etc.) must not be published under any circumstances. Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site. Pupils' work will only be published (e.g. photographs, videos, TVpresentations, web pages etc) if parental consent has been given.

ACCEPTABLE USE OF THE INTERNET

Acceptable use of the Internet is defined as, "users ensuring that access to the Internet is used solely for legal activity consistent with the aims, objectives and rules of the school".

INTERNET ACCESS

The internet is an open worldwide communication medium, available to everyone, 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 internet use through the HICS network (Hertfordshire Internet Connectivity Service) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- Internet access must be deemed a privilege rather than a right.
- Internet access requires continued demonstration of a responsible attitude and behaviour.
- Any behaviour that is rude, threatening or harmful and takes place online will not be tolerated. The same expectations of behaviour in school apply to the online world.

MANAGING THE INTERNET

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.
- Staff will preview any recommended sites, online services, software and apps before use.
- Searching for images through open search engines is 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.

INTERNET USE

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application.
- On-line gambling or gaming is not allowed.
- It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

INTERNET INFRASTRUCTURE

- Hertfordshire Local Authority has a monitoring solution via the Hertfordshire Grid for Learning where web-based activity is monitored and recorded.
- School internet access is controlled through the HICS web filtering service. For further information relating to filtering please go to http://www.thegrid.org.uk/eservices/safety/filtered.shtml
- Beechfield 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.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
- It is the responsibility of the school, by delegation to Con-Ed, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and staff are not permitted to download programs or files on school based technologies.
- If there are any issues related to viruses or anti-virus software, Con-Ed should be informed via telephone or the helpdesk.

MANAGING OTHER ONLINE TECHNOLOGIES

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking and online games websites to pupils within school.
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts

and information online.

- Our pupils are asked to report any incidents of Cyberbullying to the school.
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher.
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

SOCIAL MEDIA

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Staff ***are not*** permitted to access their personal social media accounts using school equipment at ***any time.***
- Pupils are not permitted to access their social media accounts whilst at school.
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

Primary Pupil Acceptable Use Agreement / eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, 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 my teacher immediately.
- I will only use the internet when I have permission or am supervised by a teacher.
- I will respect the privacy of others.
- I will not download software from the internet.
- I will not bring in USB flash drives, CDs or any other media from outside school unless I have been given permission.
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet anybody under any circumstance.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety.
- I will not sign up to online services until I am old enough to do so (13+ years of age in most cases).
- I understand that the sign up age for Facebook is 13 years of age. If school becomes aware that I have a Facebook account for use at school or at home they will report me to the relevant administrator.
- I will not bring a Smart Watch to school because I am not permitted to wear one during the school day.

Be Smart on the internet

Childnet International
www.childnet.com

S SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

T TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

THINK U KNOW .co.uk

www.kidsmart.org.uk

KidSMART

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Beechfield School

Gammons Lane, Watford, Herts. WD24 5TY
Telephone: 01923 221269
Fax: 01923 218699
E-mail admin@beechfield.herts.sch.uk
Web www.beechfield.herts.sch.uk

02 October 2015 **Headteacher: Miss Lisa Roberts, BEd(Hons)**

Pupil and Parent ICT and eSafety Acceptable Use

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety 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 school office.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

✂---

Parent/ carer signature

We have discussed this document with ……………………………….........(child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at Beechfield School.

We will support the school approach to online safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community or bring the school name into disrepute.

Parent/ Carer Signature …….………………….………………………….

Class …………………………………. Date ………………………………

Pupil Signature

I agree to follow the school eSafety rules in school and will remember how to keep myself safe when using ICT outside of school.

Pupil Signature ………………………….……………………….…………

Class …………………………………. Date ………………………………

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher or the Computing Leader.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, eg on a password secured laptop or memory stick.
- I will not install any hardware or software without permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and in accordance with the relevant person's image consent form or written consent of the staff member.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- Phones can be used in school as music players. It is the user's responsibility to ensure all audio output is age appropriate.
- Smart Watches are not to be worn in public areas of the school premises.
- Personal electronic devises, including mobile phones, are not to be used in public areas of the school between the hours of 8:30am and 3:30pm except in the staff room, PPA room and designated office spaces.
- Staff are not permitted to access their personal social media accounts using school equipment at any time.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional role or that of others into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

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

Signature …….. Date ……

Full Name ……..(printed)

Social Networking Staff Terms of Use

- Social media sites must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff
- Social media sites must not be used in an abusive or hateful manner
- Social media sites must not be used to discuss or advise any matters relating to school, staff, pupils or parents
- References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Headteacher
- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with
- Staff will not give out their own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- Staff are not permitted to access their personal social media accounts using school equipment at any time
- Employees should not identify themselves as a representative of the school
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally affects the employer's reputation then the employer is entitled to take disciplinary action
- Violation of these terms of use will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment
- In addition, it is strongly advised that staff do not accept or request parents as friends on any social networking site

PROFESSIONAL RESPONSIBILITIES

When using any form of ICT, including the Internet, in school and outside school

For your own protection we advise that you:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.
- Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.

You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

Developed in conjunction with the HSCB eSafety Multi-agency Panel

For HR support and guidance please contact 01438 844873
For eSafety support and guidance please contact 01438 843350

eSafety guidelines which are displayed throughout the school

MILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location) .

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend' .

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

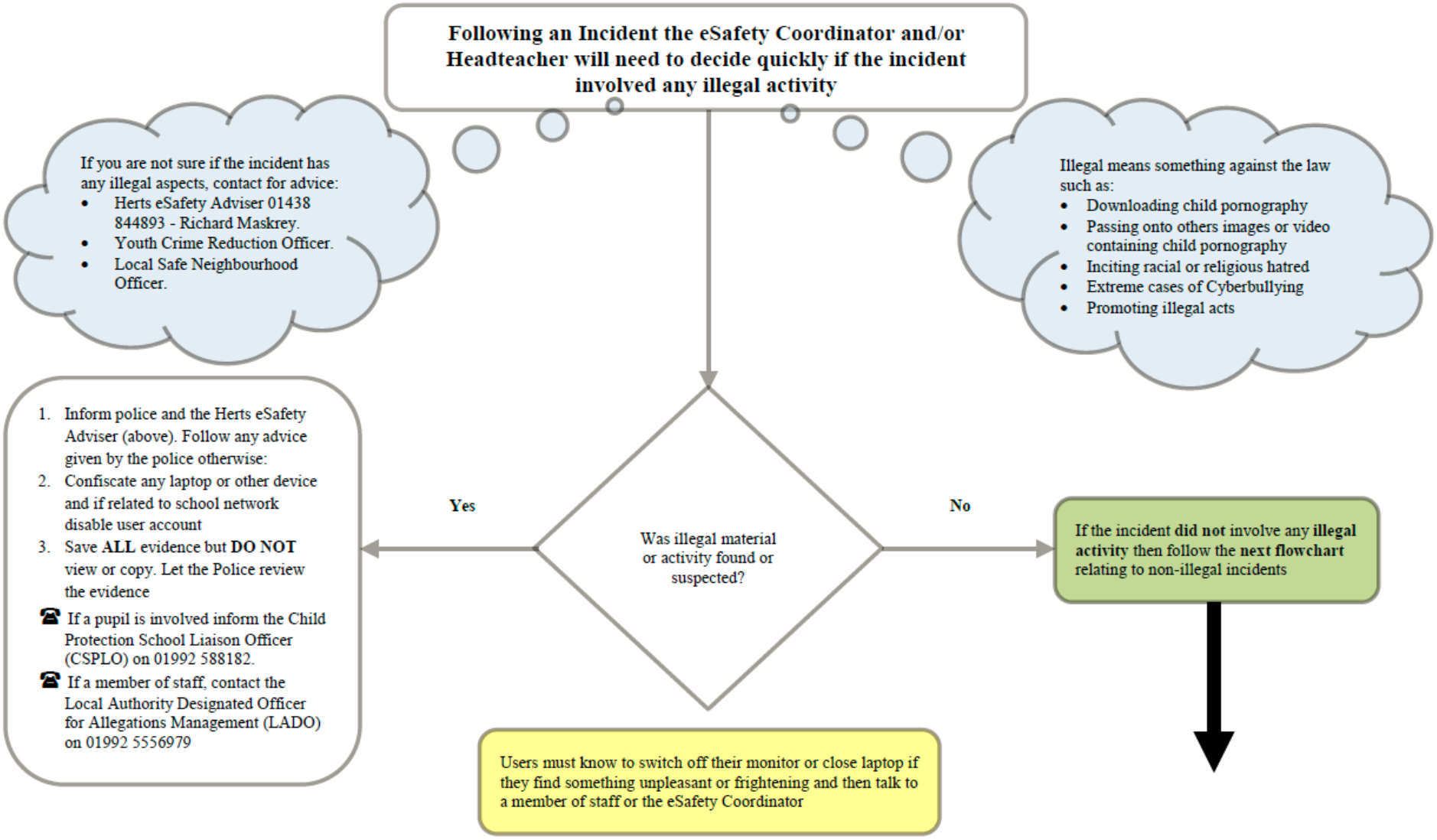
eSafety Incident Log

Details of all eSafety incidents to be recorded by ICT leader/DSP. This incident log will be monitored termly by Headteacher, Member of SLT or Chair of Governors.

Any incident involving Cyberbullying should be recorded on the 'Integrated Bullying and Racist Incident Record Form 2'.

Date & time	Name of pupil or staff member	Male or female	Room and computer/device serial number	Details of incident	Actions and reasons

Hertfordshire Flowchart to support decisions related to an illegal eSafety Incident
For Headteachers, Senior Leaders and eSafety Coordinators



If the incident **did not** involve and illegal activity then follow this flowchart

Hertfordshire Managing an eSafety Incident Flowchart

For Headteachers, Senior Leaders and eSafety Coordinators

The eSafety Coordinator and/ or Headteacher should:

- **Record in the school eSafety Incident Log**
- **Keep any evidence**

Incident could be:

- Using another person's user name and passwor
- Accessing websites which are against school policy e.g. games, social networks
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal) – talk to Herts. Anti-Bullying Adviser Karin Hutchinson 01438 844767

Did the incident involve a member of staff?

Yes

If member of staff has:

- Behaved in a way that has harmed a child, or may have harmed a child.
- Possibly committed a criminal offence against or related to a child; or
- Behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.

Contact the LADO on: 01992 556979 If the incident **does not** satisfy the criteria in **10.1.1** of the **HSCB procedures 2007**, then follow the bullet points below:

- Review the evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow the school disciplinary procedures (if deliberate) and contact Schools HR, Rachel Hurst or Christopher Williams on 01438 844933

No

Was the child the victim or the instigator?

Pupil as victim

In – school action to support pupil by one or more of the following:

- Class teacher
- eSafety Coordinator
- Senior Leader or Headteacher
- Designated Senior Person for Child Protection (DSP)
- School PCSO

Inform parents/ carer as appropriate

If the child is at risk inform CSPLO immediately

Confiscate the device, if appropriate.

Pupil as instigator

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions and/ or support based on school rules/ guidelines
- Inform parents/ carers if serious or persistent incident
- In serious incidents consider informing the CPSLO as the child instigator could be at risk
- Review school procedures/ policies to develop best practice

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator

Herts for Learning

Hertfordshire Managing an eSafety Incident Flowchart involving staff as victims

For Headteachers, Senior Leaders and eSafety Coordinators

Staff, parents, children, young people, governors and others can all become involved in an eSafety incident either as an instigator or victim. To help reduce the number of incidents we suggest that all schools and governing bodies consider the following:

Ways to prevent eSafety incidents

- Have up to-date ICT Acceptable use Policies for All users with signed user agreements. Some policies can be found on the HGfL website http://www.thegrid.org.uk/eservices/safety/policies.shtml
- Include a sentence in your Home school Agreement
  - We will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset of offend any member of the school community'
- Hold regular eSafety awareness/ update sessions for staff, governors, parents and carers
- Have an effective school complaints system which all parents, carers and others feel confident will address their concerns
- Embed eSafety throughout the curriculum and beyond

Hertfordshire Managing an eSafety Incident Flowchart involving staff as victims

For Headteachers, Senior Leaders and eSafety Coordinators