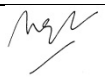
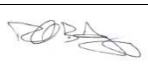
THE NOBEL SCHOOL

DOCUMENT REFERENCE	E-Safety Policy
PUBLICATION DATE	27 May 2016
AUTHORISING OFFICER	Martyn Henson
AUTHORISING OFFICER'S SIGNATURE	
DATE APPROVED BY GOVERNORS	11 May 2016
AUTHORISING GOVERNOR'S SIGNATURE	
AUTHOR/EDITOR	Steve Morley
POST	Assistant Headteacher
REVIEW DATE	27 May 2018
TARGET AUDIENCE	All Nobel Staff
STATUS	Approved

The Nobel School recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any person working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Cyber-bullying by students will be treated as seriously as any other type of bullying and will be managed through our behaviour and anti-bullying procedures which are outlined in our behaviour for learning and anti-bullying policies.

1. Legal framework

This policy has been written with due regard to the following legislation, including, but not limited to:

- Data Protection Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Racial and Religious Hatred Act 2006
- Sexual Offences Act 2003
- Communications Act 2003 (section 127)
- The Computer Misuse Act 1990 (sections 1 – 3)
- Malicious Communications Act 1988 (section 1)
- Copyright, Design and Patents Act 1988
- Public Order Act 1986 (sections 17 – 29)
- Protection of Children Act 1978 (Section 1)
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 1997

This policy also has regard to the following statutory guidance:

- DfE (2015) "Keeping Children Safe in Education"

2. Roles and Responsibility

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

The School E-Safety Coordinators are:

- Technical - Mrs Christine Crawley – Business Manager
- Safeguarding - Mr Steve Morley Asst Headteacher & Safeguarding DSL

The Designated member of the Governing Body responsible for E-Safety is:

- Mrs Sheenagh Parsons

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Coordinators
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committees

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Coordinators.
- The Headteacher and Senior Leaders are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher and the Designated Safeguarding Lead are responsible for ensuring that the E-Safety Coordinators and all other members of staff receive suitable training to enable them to carry out their e-safety roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Coordinators.

E-Safety Coordinators

- take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies and documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provide training and advice for staff
- liaise with the Local Authority
- liaise with school technical staff

- receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments (held by SSO)
- meet with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attend relevant committee of Governors
- report regularly to the Senior Leadership team

Network Manager / Technical Staff

The Network Manager, or in his/her absence, the Business Manager supported by the IT technician team, is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required safety technical requirements and any Local Authority E-Safety Guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that the filtering policy is applied
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / e-mail is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher and E-Safety Coordinators
- that monitoring software / systems are implemented and updated as agreed with the Headteacher

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement (AUA)
- that they report any suspected misuse or problem to the Headteacher and E–Safety Coordinators for investigation / action / sanction
- all digital communications with students / parents / carers should be on a professional level and only carried out using school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and Acceptable Use Agreements
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students are guided to sites that have been checked as suitable and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Leads

Should be trained in e-safety issues and be aware of the potential serious safeguarding / child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

It is important to emphasise that these are child protection issues, not technical issues simply that the technology provides additional means for child protection issues to develop.

Students

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras
- will be expected to know and understand policies on the taking / use of images and on cyber-bullying
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents/carers understand these issues through parents' evenings, letters, website, VLE and information about national / local e-safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school
- access to parents' sections of the website / VLE and online student records
- their children's personal devices in the school

3. Communicating School Policy

This policy is available from the school office for parents/carers, staff, and students to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed.

Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. We will therefore seek to provide information and awareness to parents and carers through curriculum activities, the website and high profile events and campaigns e.g. Safer Internet Day.

4. Training

Staff:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- all new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements
- the E-Safety Coordinators will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- this E-Safety Policy and its updates will be presented to and discussed by staff on inset days and in meetings
- the E-Safety Coordinators will provide advice / guidance / training to individuals as required

Governors:

Governors will be invited to take part in e-safety training / awareness sessions with particular importance for those who are members of any committee involved in technology, e-safety, health and safety and safeguarding / child protection.

This may be offered in a number of ways:

- attendance at training provided by the Local Authority / National Governors Association / or other relevant organisations
- participation in school training / information session for staff or parents

5. Making use of ICT and the Internet in School

The internet is used in school to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Some of the benefits of using ICT and the internet in schools are:

For students:

- unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries
- contact with schools in other countries resulting in cultural exchanges between students all over the world
- access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for students to interact with people that they otherwise would never be able to meet

- an enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen
- access to learning whenever and wherever convenient
- freedom to be creative
- freedom to explore the world and its cultures from within a classroom
- social inclusion, in class and online
- access to case studies, videos and interactive media to enhance understanding
- individualised access to learning

For staff:
- professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies
- immediate professional and personal support through networks and associations
- improved access to technical support
- ability to provide immediate feedback to students and parents
- class management, attendance records, schedule, and assignment tracking

For parents:
The majority of communication between the school and parents/carers is via e-mail or schoolcomms. This form of contact is considered to be more effective, reliable and economic. Text messages and letters will also inform parent/carers of details relating to attendance and behaviour.

6. Learning to evaluate Internet Content

With so much information available online it is important that students learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum.

Students will be taught:
- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The school will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites then the URL will be reported to the school E-Safety Coordinators/ICT team. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

7. Managing Information Systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by the Network Manager or in his/her absence, the Business Manager supported by the IT technician team, and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- files held on the school network will be regularly checked for viruses
- the use of user logins and passwords to access the school network will be enforced
- portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.
- termly reporting to Governors.

For more information on data protection in school please refer to our data protection policy. More information on protecting personal data can be found in section 11 of this policy.

8. E-mails

The school uses email internally for staff and students, and externally for contacting parents, and is an essential part of school communication. It is also used to enhance the curriculum by:

- initiating contact and projects with other schools nationally and internationally
- providing immediate feedback on work, and requests for support where it is needed.

Staff and students should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

8.2 School E-mail Accounts and Appropriate Use

Staff should be aware of the following when using email in school:

- staff should only use official school-provided email accounts to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people for school business
- emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications
- staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves
- the forwarding of chain messages is not permitted in school.

Students will be educated through the Computing curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

9. Published Content and the School Website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents/carers, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or students will be published, and details for contacting the school will be for the school office only. For information on the school policy on students' photographs on the school website please refer to section 9.2 of this policy.

9.2 Policy and guidance of safe use of student's photographs and work

Colour photographs and students' work bring our school to life, showcase our students' talents, and add interest to publications both online and in print that represents the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

The Nobel School believes that celebrating the achievement of children in school is an important part of their learning experience and personal development. Taking photographs and videos of students for internal display and displaying student work for educational use enables us to celebrate individual and group successes as a school community.

However, we would also like to use photographs and videos of the school and its students externally for promotional purposes (in the public domain) and in order to promote the good educational practice of the school but in accordance with the Data Protection Act 1998 we will only do this with parent/carer consent. On admission to the school parents/carers will be asked to sign a permissions agreement which incorporates digital/video permissions.

By signing this form parents/carers will be consenting to the use of images of their son/daughter being used in the following outlets:

- all school publications
- on the school website
- in newspapers as allowed by the school
- in videos made by the school or in class for school projects

The form covers consent for the duration of their child's time at the school. Once the student leaves the school, photographs and videos may be archived within the school or may be used for promotional purposes e.g. in the school prospectus.

Students' full names may be published externally with their photographs e.g. in a local press release.

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

- parental consent must be obtained for external/promotional use. See above
- electronic and paper images will be stored securely
- images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the students
- for public documents, including in newspapers, full names will not be published alongside images of the child without prior consent. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only and not posted online for public viewing
- students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in
- any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the students. For more information on safeguarding in school please refer to our school safeguarding and child protection policy.

9.3 Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs.

9.4 Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the Computing curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- students are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online
- any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use
- official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run with the approval of a member of staff and will be moderated by a member of staff
- students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and students to remember that they are representing the school at all times and must act appropriately
- safe and professional behaviour of staff online will be discussed at staff induction.

10. Mobile Phones and Personal Devices

While mobile phones and personal communication devices are common place in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

- they can make students and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material
- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged, or lost
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school therefore adopts a zero tolerance Electronic Device Policy for students during the school day (the sixth form are permitted to use their I-pads if the staff member allows):

- phones and electronic devices (including headphones) will be confiscated and given to student support for storage prior to being given back to the student or parent
- the parents/carer will be contacted and asked to collect the phone/device according to the Behaviour for learning policy
- the incident will be logged on our behaviour management system and a detention will probably be required to be served
- any student who refuses to hand over the complete phone / device when requested may be removed from the lesson. The behaviour for learning policy will then apply
- in circumstances where there is a suspicion that material on a phone is unsuitable the phone will be inspected by staff and then handed over to the Police for further investigation.

We do however, understand that a parent/carer may wish for their son to have a mobile phone for their journey to and from school. In this situation, and in order to reduce the risk of having a phone confiscated, a student can hand their phone/device into the pastoral office.

Emergencies:

- If a student needs to contact his parents/carers they will be allowed to use a school phone.

- If parents/carers need to contact their son(s) urgently they should phone the school office and a message will be relayed promptly.

Responsibility:

- The Nobel School accepts no responsibility whatsoever for theft, loss or damage relating to phones/devices including those handed in/confiscated.
- The Nobel School will, usually, not investigate theft, loss or damage relating to phones/devices.

Staff

- Under no circumstances should staff use their own personal devices to contact students or parents either in or out of school time unless in an emergency.
- Staff are not permitted to take photos or videos of students without SLT approval. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this; where feasibly possible. Staff will be expected to delete any photos taken on personal devices as soon as the photos are uploaded onto school ICT equipment. Any such photos should not be published online except via the school website, Facebook or Twitter accounts.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.
- Any breach of school policy may result in disciplinary action against that member of staff.

11. Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the anti-bullying policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

All alleged, or proven, incidents of cyber bullying will be dealt with using the Nobel anti-bullying policy and procedures. Logs of all such events are kept in the Pastoral Office; cyber bullying log will be separate from other bullying logs.

If an allegation of bullying does come up, the school will:

- take it seriously
- act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- record and report the incident, according to policy
- provide support and reassurance to the victim, according to policy
- make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if the bully refuses or is unable to remove it. They may have their internet access suspended in school.

Repeated bullying may result in a fixed-term exclusion.

All alleged, or proven, incidents of cyber bullying will be dealt with using the Nobel anti-bullying policy and procedures. Logs of all such events are kept in the Pastoral Office; cyber bullying log will be separate from other bullying logs.

12. Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

13. Protecting Personal Data

The Nobel School believes that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure

- ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection read the school's data protection policy.

14. Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or disturbing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the user or the nature of those activities. The school believes that these activities would be inappropriate in our school context:

- pornography
- promotion of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- using school systems to run a private business
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- infringing copyright
- revealing or publicising confidential or proprietary information e.g. financial, personal information, data bases, computer / network access codes and passwords
- creating or propagating computer viruses or other harmful files
- unfair usage
- on-line gaming, educational and non-educational
- on-line gambling
- use of social media without permission
- use of messaging apps without permission
- use of videoing broadcasting or YouTube without permission

14.1 Responding to incidents of misuse

Illegal incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the flow chart attached to this policy. (see appendix 1.)

Other incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. (see appendix 2, 3.)

In the event of suspicion, all steps in this procedure should be followed:

- more than one senior member of staff should be involved in the process. This is vital to protect individuals if accusations are subsequently reported
- the procedure should be conducted using a designated computer that will not be used by students and if necessary can be taken off site by the police should the need arise. The same computer should be used for the duration of the process
- relevant staff should have appropriate internet access to conduct the procedure, and sites and content visited closely monitored and recorded to provide further protection
- the URL of any site containing the alleged misuse and the nature of the content causing concern should be recorded. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. This may be printed, signed and attached to the form (except in cases of child sexual abuse)
- once fully investigated the group should judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following;

    Internal response or discipline procedures

    Involvement by Local Authority or national / local organisations (as relevant)

    Police involvement and / or action

- if content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

    Incidents of 'grooming' behaviour

    The sending of obscene materials to a child

    Adult material which potentially breaches the Obscene Publications Act

    Criminally racist material

    Other criminal conduct, activity or material

• isolate the computer in question as best you can. Any changes to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

School actions and sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather illegal misuse. It is important that any incidents are dealt with as soon as possible in an appropriate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures and could include:

Students:

- referral to class teacher / tutor
- referral to Head of Department / Head of Year
- referral to E-Safety Co-ordinator(s)
- referral to Line Manager
- referral to Headteacher
- referral to the Police
- referral to technical support staff for action re filtering / security etc.
- informing parents / carers
- removal of network / internet access rights
- risk assessment
- warning
- detention
- fixed Term Exclusion
- permanent Exclusion

Staff:

- referral to Line Manager
- referral to Headteacher
- referral to Local Authority / HR
- referral to technical support staff for action re filtering etc.
- risk assessment
- warning
- referral to agency / counselling
- suspension
- disciplinary action
- referral to the Police
- dismissal

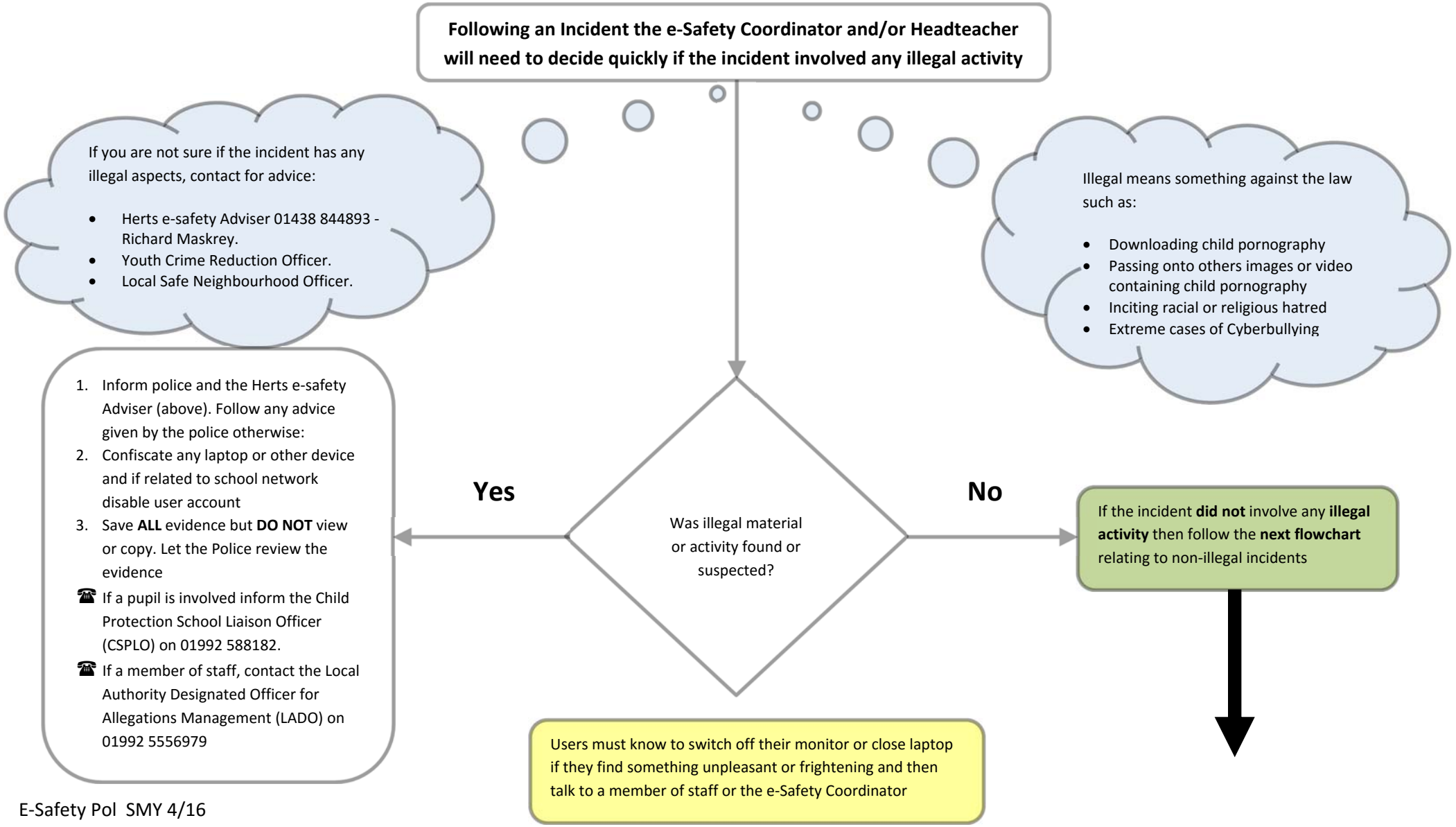
A log of all alleged, or proven, e-safety incidents will be kept in the Pastoral Office.

All alleged, or proven, incident of cyber bullying will be dealt with using the Nobel anti-bullying policy and procedures. Logs of all such events are kept in the Pastoral Office; cyber bullying log will be separate from other bullying logs.

APPENDIX 1:

Nobel Flowchart to support decisions related to an illegal e-Safety Incident

For Headteachers, Senior Leaders and e-Safety Coordinators



APPENDIX 2:

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

Nobel Managing an e-Safety Incident Flowchart

For Headteachers, Senior Leaders and e-Safety Coordinators

The e-safety Coordinator and/ or Headteacher should:

- **Record in the school e-safety Incident Log**

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 school HR, Rachel Hurst or Christopher Williams on 01438 844933

No

Incident could be:

- Using another person's user name and password
- 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

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
- e-safety Coordinator
- Senior Leader or Headteacher
- Designated Senior Person for Child Protection (DSP)
- School PCSO

Inform parents/ carer as 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 e-Safety Coordinator

APPENDIX 2: Nobel Managing an e-Safety Incident Flowchart involving staff as victims

For Headteachers, Senior Leaders and e-Safety Coordinators

All incidents should be reported to the Headteacher and/ or Governors who will:

- Record in the school e-Safety Incident Log
- Keep any evidence – printouts and/ screen shots
- Use the 'Report Abuse' button, if appropriate
- Consider including the Chair of Governors and/ or reporting the

If you feel unable to report an incident to your HT you could talk to a member of SLT or contact the Hertfordshire e-Safety Adviser 01438 844893 richard.maskrey@hertsforlearning.co.uk

Parents/ carers as instigators

Follow some of the steps below:

- Contact the person and invite into school and discuss using some of the examples below:
  - You have become aware of discussions taking place online…
  - You want to discuss this
  - You have an open door policy so disappointed they did not approach you first
  - They have signed the Home School Agreement which clearly states …
  - Request the offending material be removed.
- If this does not solve the problem:
  - Consider involving the Chair of Governors

Staff as instigator

Follow some of the steps below:

- Contact Schools HR for initial advice and/ or contact Schools e-Safety Adviser in all serious cases this is the first step.
- Contact the member of staff and request the offending material be removed immediately. (In serious cases you may be advised not to discuss the incident with the staff member)
- Refer to the signed ICT Acceptable Use Agreement, Professional Code of Conduct and consider if this incident has an impact on the Contract of Employment of the member of staff.

Pupils as instigators

Follow some of the steps below:

- Identify the pupil involved
- Ask pupil to remove offensive material. Refer to the signed Acceptable Use Agreement.

If the perpetrator refuses to remove the material and is under 13 contact the Social Network who will close the account

- Take appropriate actions in line with school policies/ rules
- Inform parents/ carers if serious or persistent incident

For serious incidents or further advice:

- Inform your Local Police Neighbourhood Team
- Anti-Bullying Adviser Karin Hutchinson 01438 844767

Further contact to support staff include:

- District School Effectiveness Adviser DSEA
- Schools e-Safety Adviser
- Schools HR
- School Governance
- Hertfordshire Police
- HCC Legal Helpline 01992 555536

The HT or Chair of Governors can be the single point of contact to coordinate responses.