North Leamington School
E–Safety Policy

November 2015

CORE Purpose

1. **Commitment:** North Leamington School believes that the use of information and communication technologies in schools brings great benefits. Recognising the e-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

2. **Opportunities:** In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

3. **Respect:** e-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

4. **Excellence:** NLS must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. NLS must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

NLS commitment

5. Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, students and members of the wider school community. It is crucial that all settings are aware of the offline consequences that online actions can have.

6. NLS is aware of their legal obligation to safeguard and protect children on and offline and the accountability of these decisions will sit with the Headteacher and the Governing Body.

7. The e-Safety policy is essential in setting out how NLS plans to develop and establish its e-Safety approach and to identify core principles which all members of the NLS school community need to be aware of and understand.

Reviewing the policy

8. The e-Safety Policy is part of many different school policies including the, Child Protection, Anti-Bullying Policy and Engagement for Learning Policy. NLS will

consult with staff, parents, governors and students in deciding and creating the policy.

9. It is recommended as best practice that all schools appoint an e-Safety Coordinator to lead on e-Safety. The person who is appointed does not need to have vast technical knowledge; however it would be helpful if they had some basic understanding of ICT. The SAHT and the School PCSO will take school responsibility for e-safety.

10. NLS Designated Child Protection Coordinator (DCPC) will need to be aware of e-Safety training and resources and be available should any child wish to disclose information regarding an online incident. Therefore it may be an idea to elect them as e-Safety representative. However another member of staff may be selected. The DCPC must be made aware of any disclosures, incidents or Child Protection concerns. The Senior Leadership Team and Governing Body must be involved and should review the e-Safety policy annually and monitor its impact. They will also need to ensure that they take responsibility for revising the e-Safety policy and practice where necessary (such as after an incident or change in national legislation).

11. The Headteacher and Governing body have a legal responsibility to safeguard children and staff and this includes online activity.

a) The school has appointed an e–Safety Coordinator.
b) The e–Safety Policy and its implementation will be reviewed annually.
c) Our e–Safety Policy has been written by the school, building on the WCC e–Safety Policy and government guidance.
d) Our School Policy has been agreed by the Senior Leadership Team and approved by governors.

NLS e-Safety Coordinator is **Mrs Nicola Holt**………………………………

Policy approved by Headteacher: ………………………………..… Date: ……………

Policy approved by Governing Body: …………………………….. (Chair of Governors)

Date: ……………

The date for the next policy review is **Autumn Term 2017**

Teaching and learning

Why is Internet use important?

12. The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

a) Internet use is part of the statutory curriculum and is a necessary tool for learning.
b) The Internet is a part of everyday life for education, business and social interaction.
c) The school has a duty to provide students with quality Internet access as part of their learning experience.

d) Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
e) The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school’s management functions.
f) Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

13. A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

14. Benefits of using the Internet in education include:
a) access to worldwide educational resources including museums and art galleries
b) inclusion in the National Education Network which connects all UK schools
c) educational and cultural exchanges between students worldwide
d) vocational, social and leisure use in libraries, clubs and at home
e) access to experts in many fields for students and staff
f) professional development for staff through access to national developments, educational materials and effective curriculum practice
g) collaboration across networks of schools, support services and professional associations
h) improved access to technical support including remote management of networks and automatic system updates
i) exchange of curriculum and administration data with appropriate agencies
j) access to learning wherever and whenever convenient.

How can Internet use enhance learning?

15. Increased computer numbers and improved Internet access may be provided but its impact on students learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Students need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Methods to detect plagiarism may need to be developed.

a) The school’s Internet access will be designed to enhance and extend education.
b) Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
c) The school will ensure that the copying and subsequent use of Internet-derived materials by staff and students complies with copyright law.
d) Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of students.
e) Staff should guide students to online activities that will support the learning outcomes planned for the student’s age and ability.
f) Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
g) Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will students learn how to evaluate Internet content?

16. The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

17. Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy, etc., provide an opportunity for students to develop skills in evaluating Internet content. For example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

a) Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
b) Students will use age-appropriate tools to research Internet content.
c) The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems

How will information systems security be maintained?

18. It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and students.

19. ICT security is a complex issue which cannot be dealt with adequately within this document.

20. Local Area Network (LAN) security issues include:
a) Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
b) Users must take responsibility for their network use.
c) Workstations should be secured against user mistakes and deliberate actions.
d) Servers must be located securely and physical access restricted.
e) The server operating system must be secured and kept up to date.
f) Virus protection for the whole network must be installed and current.
g) Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.
h) The security of the school information systems and users will be reviewed regularly.
i) Virus protection will be updated regularly.
j) Personal data sent over the Internet or taken off site will be encrypted.
k) Portable media may not be used without specific permission followed by an anti-virus/malware scan.
l) Unapproved software will not be allowed in work areas or attached to email.
m) Files held on the school's network will be regularly checked.
n) The ICT coordinator/network manager will review system capacity regularly.

o) The use of user logins and passwords to access the school network will be enforced.

How will email be managed?

21. Email is an essential means of communication for both staff and students. Directed email use can bring significant educational benefits; interesting projects between schools and in different continents can be created, for example.

22. The implications of email use for the school and students need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to students that bypass the traditional school boundaries.

23. A central question is the degree of responsibility that can be delegated to individual students as once email is available it is difficult to control. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible.

24. In the school context (as in the business world), email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of students and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents/carers, students and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

25. The use of email identities such as john.smith@northleamington.co.uk generally needs to be avoided for younger students, as revealing this information could potentially expose a child to identification by unsuitable people. Email accounts should not be provided which can be used to identify both a student's full name and their school. NLS limits students to email accounts approved and managed by the school. When using external providers to provide students with email systems, schools must pay close attention to the sites terms and conditions as some providers have restrictions of use and age limits for their services.

a) Students may only use approved email accounts for school purposes.
b) Students must immediately tell a designated member of staff if they receive offensive email.
c) Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
d) Staff will only use official school provided email accounts to communicate with students and parents/carers, as approved by the Senior Leadership Team.
e) Access in school to external personal email accounts can be blocked.
f) Excessive social email use can interfere with learning and will be restricted.
g) Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
h) The forwarding of chain messages is not permitted.
i) Staff should not use personal email accounts during school hours or for professional purposes.

How will published content be managed?

26. NLS has created an excellent website and communication channels, which inspire students to publish work of a high standard. The website celebrates students' work, promotes the school and publishes resources for projects. Editorial guidance helps reflect the school's requirements for accuracy and good presentation.

27. Sensitive information about schools and students could be found in a newsletter but a school's website is more widely available. Publication of any information online should always be considered from a personal and school security viewpoint.

- The contact details on the website should be the school address, email and telephone number. Staff or students' personal information must not be published.
- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can students' images or work be published?

28. Still and moving images and sound add liveliness and interest to a publication, particularly when students can be included. Nevertheless the security of staff and students is paramount. Although common in newspapers, the publishing of students' names with their images is not acceptable. Published images could be reused, particularly if large images of individual students are shown.

29. Strategies include using relatively small images of groups of students and possibly even using images that do not show faces at all. "Over the shoulder" can replace "passport style" photographs but still convey the educational activity. Personal photographs can be replaced with self-portraits or images of students' work or of a team activity. Students in photographs should, of course, be appropriately clothed.

30. Images of a student should not be published without the parent's or carer's written permission. Some schools ask permission to publish images of work or appropriate personal photographs on entry, some once a year, others at the time of use.

31. Students also need to be taught the reasons for caution in publishing personal information and images online

a) Images or videos that include students will be selected carefully and will not provide material that could be reused.
b) Students' full names will not be used anywhere on the website, particularly in association with photographs.
c) Written permission from parents or carers will be obtained before images/videos of students are electronically published.
d) Students work can only be published with their permission or the parents.
e) Written consent will be kept by the school where students' images are used for publicity purposes, until the image is no longer in use.
f) The school will have a policy regarding the use of photographic images of children which outlines policies and procedures (local authority document).

How will social networking, social media and personal publishing be managed?

32. Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

33. For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Students should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

34. All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

35. Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

36. Additional guidance and considerations for schools around this topic (including a checklist and risk assessment templates) can be found in the “Using Social Media and Technology in Educational Settings” document.

a) The school will control access to social media and social networking sites.
b) Students will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
c) Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
d) Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for student use on a personal basis.
e) Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
f) Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
g) All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

h) Newsgroups will be blocked unless a specific use is approved.
i) Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
j) Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

How will filtering be managed?

37. Levels of Internet access and supervision will vary according to the student's age and experience. Access profiles must be appropriate for all members of the school community. Older secondary students, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. Systems to adapt the access profile to the student's age and maturity are available.

38. Access controls fall into several overlapping types (commonly described as filtering):

a) Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
b) A walled garden or "allow list" restricts access to a list of approved sites. Such lists inevitably limit students' access to a narrow range of content.
c) Dynamic content filtering examines web page content or email for unsuitable words.
d) Keyword lists filter search engine searches and URLs for inappropriate results and web addresses. Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject rated pages exceeding a threshold.
e) URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate student access.
f) Key loggers record all text sent by a workstation and analyse it for patterns.

39. Thousands of inappropriate sites are created each day and many change URLs to confuse filtering systems. It is the Senior Leadership Team's responsibility to ensure appropriate procedures are in place and all members of staff are suitably trained to supervise Internet access.

40. It is important to recognise that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. mobile phone).

41. Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using internet access and that Acceptable Use Policies are in place. In addition, Internet Safety Rules should be displayed, and both children and adults should be educated about the risks online. There should also be an Incident Log to report breaches of filtering or inappropriate content being accessed. Procedures need to be established to report such incidents to parents and outside agencies where appropriate.

42. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF, Warwickshire Police or CEOP.

43. Websites which staff and students believe should be blocked centrally should be reported to the ICT Helpdesk. Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the students. Often this will mean checking the websites, search results, etc., just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

a) The school's broadband access will include filtering appropriate to the age and maturity of students.
b) The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all students) will be aware of this procedure.
c) If staff or students discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
d) The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
e) Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
f) The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
g) Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Warwickshire Police or CEOP
h) The school's access strategy will be designed by educators to suit the age and curriculum requirements of the students, with advice from network managers.

How are emerging technologies managed?

44. Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details.

45. New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a student using a phone to video a teacher's reaction in a difficult situation.

46. Schools should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance text messaging via mobile phones is a frequent activity for many students and families; this could be used to communicate a student's absence or send reminders for exam coursework. There are dangers for staff however if personal phones are used to contact students and therefore a school owned phone should be issued.

47. The inclusion of inappropriate language or images is difficult for staff to detect. Students may need reminding that such use is inappropriate and conflicts with school policy. Abusive messages should be dealt with under the school's behaviour and/or anti-bullying policies.

a) Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
b) Students will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

How should personal data be protected?

48. The quantity and variety of data held on students, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

49. The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

50. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

51. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

How will Internet access be authorised?

52. The school should allocate Internet access to staff and students on the basis of educational need. It should be clear who has Internet access and who has not. Authorisation is generally on an individual basis in a secondary school. In a primary school, where pupil usage should be fully supervised, all students in a class could be authorised as a group.

53. Normally most students will be granted Internet access; it may be easier to manage lists of those who are denied access. Parental permission should be encouraged for Internet access in all cases — a task that may be best organised annually when students' home details are checked and as new students join or as part of the Home-School agreement. If schools do request parental consent for internet access it is essential to record this data. Schools must be aware that students should not be prevented from accessing the internet unless the parents have specifically denied permission or the child is subject to a sanction as part of the Engagement for Learning policy.

a) The school will maintain a current record of all staff and students who are granted access to the school's electronic communications.
b) All staff will read and sign the 'Staff Information Systems Code of Conduct' or School Acceptable Use Policy before using any school ICT resources.
c) Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
d) All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
e) Parents will be informed that students will be provided with supervised Internet access appropriate to their age and ability.
f) When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
g) Secondary students will apply for Internet access individually by agreeing to comply with the School e–Safety Rules or Acceptable Use Policy.

How will risks be assessed?

54. As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will need to address the fact that it is not possible to completely remove the risk that students might access unsuitable materials via the school system. It is wise to include a disclaimer, an example of which is given below.

55. Risks can be considerably greater where tools are used which are beyond the school's control such as most popular social media sites. Guidance and considerations for staff around this topic (including a checklist and sample risk assessment templates) can be found in the "Using Social Media and Technology in Educational Settings" document.

a) The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor WCC can accept liability for the material accessed, or any consequences resulting from Internet use.
b) The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
c) The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Warwickshire Police.
d) Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

56. Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However it is also important to consider the risks associated with the way these technologies can be used. An e-Safety Policy should recognise and seek to develop the skills that children and young people need when communicating and using technologies enabling them to keep safe and secure and act with respect for others.

57. e-Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about students and in developing trust so that issues are reported.

58. Staff should also help develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the school Designated Child Protection Coordinator.

59. Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, schools should determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible, after contacting the Children Safeguarding Team or e-Safety officer, if the offence is deemed to be out of the remit of the school to deal with.

a) All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
b) The e-Safety Coordinator will record all reported incidents and actions taken in the Student e-portfolio and in any relevant areas e.g. Bullying or Child protection log.
c) The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
d) The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
e) The school will inform parents/carers of any incidents of concern as and when required.
f) After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
g) Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguarding Team or e-Safety Officer and escalate the concern to the Police
h) If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer at WCC ICTDS.

How will e–Safety complaints be handled?

60. Parents, teachers and students should know how to use the school's complaints procedure. The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. E-Safety incidents may have an impact on students, staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

61. A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions may then be required, which should be linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator or e–Safety Coordinator. Advice on dealing with illegal use can, when deemed necessary, be discussed with Warwickshire Police

a) Complaints about Internet misuse will be dealt with under the School's complaints procedure.
b) Any complaint about staff misuse will be referred to the Headteacher.
c) All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
d) Students and parents will be informed of the complaints procedure.
e) Parents and students will need to work in partnership with the school to resolve issues.
f) All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
g) Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguarding Team to establish procedures for handling potentially illegal issues.
h) Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
i) All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How will Cyberbullying be managed?

62. Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DfE 2007

63. Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

64. It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

65. There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

a) every school must have measures to encourage good behaviour and prevent all forms of bullying amongst students. These measures should be part of the school's behaviour policy which must be communicated to all students, school staff and parents

b) gives Headteachers the ability to ensure that students behave when they are not on school premises or under the lawful control of school staff.

66. Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on.

67. Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed they should seek assistance from the police.

68. For more information please read "Preventing and Tackling Bullying: Advice for School Leaders, Staff and Governing Bodies" http://www.education.gov.uk/aboutdfe/advice/f0076899/preventing-and-tackling-bullying

69. DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

a) Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and Engagement for Learning.

b) There are clear procedures in place to support anyone in the school community affected by cyberbullying.

c) All incidents of cyberbullying reported to the school will be recorded.

d) There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

e) Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.

f) The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

g) Students, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

h) Sanctions for those involved in cyberbullying may include:

i. The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.

ii. Internet access may be suspended at school for the user for a period of time. Other sanctions for students and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.

iii. Parent/carers of students will be informed.

iv. The Police will be contacted if a criminal offence is suspected.

How will Learning Platforms be managed? (by Miss Sunita Chandegra)

70. An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, students and parents, as well as support for management and administration. It can enable students and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and students can develop online and secure e-portfolios to showcase examples of work.

71. The Learning Platform/Environment (LP) must be used subject to careful monitoring by the Senior Leadership Team (SLT). As usage grows throughout the school then more issues could arise regarding content, inappropriate use and behaviour online by users. The SLT has a duty to annually review and update the policy regarding the use of the Learning Platform, and all users must be informed of any changes made.

a) SLT and staff will regularly monitor the usage of the LP by students and staff in all areas, in particular message and communication tools and publishing facilities.
b) Students/staff will be advised about acceptable conduct and use when using the LP.
c) Only members of the current pupil, parent/carers and staff community will have access to the LP.
d) All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
e) When staff, students etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
f) Any concerns about content on the LP may be recorded and dealt with in the following ways:
   i. The user will be asked to remove any material deemed to be inappropriate or offensive.
   ii. The material will be removed by the site administrator if the user does not comply.
   iii. Access to the LP for the user may be suspended.
   iv. The user will need to discuss the issues with a member of SLT before reinstatement.
   v. A student’s parent/carer may be informed.
g) A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
h) Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

Communication Policy

How will the policy be introduced to students?

72. Many students are very familiar with the culture of mobile and Internet use and it is wise to involve them in designing the School e–Safety Policy, possibly through a student council. As students’ perceptions of the risks will vary; the e–Safety rules may need to be explained or discussed.

73. The student and parent agreement form should include a copy of the school e–Safety rules appropriate to the age of the student.

74. Consideration must be given as to the curriculum place for teaching e–Safety. This could be as an ICT lesson activity, part of the pastoral programme or part of every subject whenever students are using the Internet.

75. Useful e–Safety programmes include:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Orange Education: www.orange.co.uk/education
- Safe: www.safesocialnetworking.org

a) All users will be informed that network and Internet use will be monitored.
b) An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst students.
c) Student instruction regarding responsible and safe use will precede Internet access.
d) An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
e) E–Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
f) E-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
g) Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
h) Particular attention to e-Safety education will be given where students are considered to be vulnerable.

How will the policy be discussed with staff?

76. It is important that all staff feel confident to use new technologies in teaching and the School e–Safety Policy will only be effective if all staff subscribe to its values and methods.

77. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

78. All staff must understand that the rules for information systems misuse for WCC employees are specific and that instances resulting in disciplinary procedures and dismissal have occurred. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their line manager to avoid any possible misunderstanding.

79. Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside of the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information.

80. ICT use is widespread and all staff including administration, midday supervisors, caretakers, governors and volunteers should be included in awareness raising and training. Induction of new staff should include a discussion about the school e–Safety Policy.

a) The e–Safety Policy will be formally provided to and discussed with all members of staff.
b) To protect all staff and students, the school will implement Acceptable Use Policies.
c) Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
d) Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
e) Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
f) The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the students.
g) All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted?

81. Internet use in students' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, students may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to check whether their child's use elsewhere in the community is covered by an appropriate use policy.

82. One strategy is to help parents to understand more about ICT , perhaps by running courses and parent awareness sessions (although the resource implications will need to be considered).

a) Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
b) A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.
c) Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.
d) Parents will be encouraged to read the school Acceptable Use Policy for students and discuss its implications with their children.
e) Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.
f) Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
g) Interested parents will be referred to organisations listed in the "e–Safety Contacts and References section".

E-Safety Contacts and References

a) **CEOP** (Child Exploitation and Online Protection Centre): www.ceop.police.uk

b) **ChildLine:** www.childline.org.uk

c) **Childnet:** www.childnet.com

d) **Click Clever Click Safe Campaign:** http://clickcleverclicksafe.direct.gov.uk

e) **Cybermentors:** www.cybermentors.org.uk

f) **Digizen:** www.digizen.org.uk

g) **Internet Watch Foundation** (IWF): www.iwf.org.uk

h) **Kidsmart**: www.kidsmart.org.uk

i) **Schools Broadband Service Desk -** Help with filtering and network security: www.eiskent.co.uk Tel: 01622 206040

j) **Schools e–Safety Blog:** www.kenttrustweb.org.uk?esafetyblog

k) **Teach Today:** http://en.teachtoday.eu

l) **Think U Know website**: www.thinkuknow.co.uk

m) **Virtual Global Taskforce** — Report Abuse: www.virtualglobaltaskforce.com