NEALE-WADE

Neale-Wade Academy

E–Safety Policy 2016-2018

1

360 degree safe

COMMITTED TO SAFETY ONLINE

Contents

1.1 Authoring and review of policy

The e-Safety Policy is part of many different schools policies including the ICT Policy, Child Protection or Safeguarding Policy, Anti-Bullying and School Development Plan and should relate to other policies including those for behaviour, for personal, social and health education (PSHE) and for citizenship. Policy construction provides a method to review practice - in this case the use of technology and its benefits and risks. The more that staff, parents, governors and students are involved in deciding and creating the policy, the more effective it will be.

- The school has appointed an e–Safety Coordinator.
- The e–Safety Policy and its implementation will be reviewed annually.
- Our e–Safety Policy has been written by the school, building on a range of relevant documentation and government guidance.
- Our School Policy has been agreed by the Senior Leadership Team and approved by governors**.**

The School e-Safety Coordinator is Stephen Bradbury

Policy approved by Principal:

…………………………………………...

Date: ………………………………….

Policy approved by Governing Body: (Chair of Governors)

…………………………………………...

Date: ………………………………….

1.2 Teaching and learning

1.2.1 Why is Internet use important?

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.

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Care needs to be taken to ensure that students without access at home are directed to use available College resources and given every support to do so.
- Students use the Internet widely outside school and need to learn how to evaluate Internet-based information and to take care of their own safety and security.
- 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.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

1.2.2 How does Internet use benefit education?

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

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries
- inclusion in the National Education Network which connects all UK schools; educational and cultural exchanges between Students worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for Students and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with county, DfE and other relevant agencies access to learning wherever and whenever convenient.

1.2.3 How can Internet use enhance learning?

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.

- The school's Internet access will be designed to enhance and extend education.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and Students complies with copyright law.
- Staff should guide Students to online activities that will support the learning outcomes planned for the Students' age and ability.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

1.2.4 How will Students learn how to evaluate Internet content?

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.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy 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.

- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will use age-appropriate tools to research Internet content.
- 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.

1.3 Managing Information Systems

1.3.1 How will information systems security be maintained?

Our Schools in-house IT Department and support company (Currently RM) maintain school systems security.

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For CCC staff, flouting the Acceptable use policy is regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) security issues include:

- Decisions on WAN security are made on a partnership between schools and CCC
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- System capacity will be regularly reviewed.
- The use of user logins and passwords to access the school network will be enforced.

1.3.2 How will email be managed?

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

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.

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.

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.

The use of email identities such as john.smith@school.cambs.sch.uk generally needs to be avoided for younger Students, as revealing this information could potentially expose a child to identification by unsuitable people.

Neale-Wade students should only use email accounts approved and managed by the College. Currently all students use an official educational Google apps account.

- Students may only use approved email accounts for school purposes.
- Students must immediately tell a member of staff if they receive offensive email.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with Students and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning will be restricted.
- Email sent to external organisations should be written carefully and to the same standards as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Neale-Wade will continue to use a parental contact form to enable reporting wellbeing and pastoral issues. This will be managed by designated and trained staff.
- Staff should not use personal email accounts during school hours or for professional purposes.

1.3.3 How will published content be managed?

Many schools have created excellent websites and communication channels, which inspire Students to publish work of a high standard. Websites can celebrate Students' work, promote the school and publish resources for projects. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

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. Material such as staff lists or a school plan may be better published in the school handbook or on a secure part of the website which requires authentication.

The contact details on the website should be the school address, email and telephone number. Staff or students' personal information must not be published.

Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)

The Principal 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.

1.3.4 Can students’ images or work be published?

Images, Videos 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.

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.

Images of a student should not be published without the parent’s or carer’s written permission.

Students also need to be taught the reasons for caution in publishing personal information and images online (see section 2.3.6).

- Images or videos that include students will be selected carefully and will not provide material that could be reused.
- Student names will not be published with a photo that clearly identifies who they are.
- No photo will be published online that has fewer than 3 students
- Written permission from parents or carers will be obtained before images/videos of Students are electronically published.
- Students’ work can only be published with their permission or the parents.
- Written consent will be kept by the school where Students’ images are used for publicity purposes, until the image is no longer in use – permission recorded in SIMS.

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

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.

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.

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

It is mandatory that all staff confirm in writing that they have read Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings. This provides clear and direct guidance for the use of social media that all staff should follow.

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.

The school will control access to social media and social networking sites through our county council provided internet filtering solution.

- Students will be advised as part of their ICT curriculum 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.
- The expectation of Neale-Wade is that staff do not have students as 'friends' on social networking sites. We are aware that some members of staff have children that are students. We would advise that if you do have your child as a 'friend' that privacy settings are set appropriately to prevent any issues of professional misconduct.
- 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.
- 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. Staff should make use of the College provided VLE and related tools for such purposes.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- 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. Student will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

- 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.
- 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.
- 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 Statement.

1.3.6 How will filtering be managed?

The Schools in-house IT department alongside Cambridgeshire County ICT Services monitor and maintain school systems filtering.

- The school’s broadband access will include filtering appropriate to the age and maturity of Students.
- 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.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as CEOP.

1.3.7 How will videoconferencing be managed?

Videoconferencing enables users to see and hear each other between different locations. This ‘real time’ interactive technology has many uses in education.

The College has access to Skype for Business which includes videoconferencing capabilities.

1.3.8 How are emerging technologies managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within school systems. Online communities can also be one way of encouraging a disaffected student to keep in touch.

The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites and other online tools such as Facebook, YouTube, Skype and Twitter. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often possible. 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.

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.

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. Staff should not communicate with students / parents using their personal phone. A school owned phone will be issued for trips and residential activities.

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.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Students are not allowed to use mobile phones on site unless it is part of an approved educational activity.
- Students will be instructed about safe and appropriate use of personal devices both on and off site.

- **1.3.9 How should personal data be protected?**

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.

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

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.

Schools will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

For advice and guidance relating to a contravention of the Act, contact the Principal as the College in now directly registered with the DP Commissioner.

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

1.4 Policy Decisions

1.4.1 How will Internet access be authorised?

The school should allocate Internet access to staff and students on the basis of educational need. Students will be given appropriate access on the basis of an educational need unless a parent opts out.

- All staff will read and agree to the School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy (as part of the Home-School agreement) for student access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to agree to the Acceptable Use Policy.
- 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 student(s).

1.4.2 How will risks be assessed?

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 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 CCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- 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.
- 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 the Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

1.4.3 How will the school respond to any incidents of concern?

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.

e-Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Staff 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.

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 Safeguard Team or e-Safety officer, if the offence is deemed to be out of the remit of the school to deal with.

- 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).
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline / behaviour policy.
- The school will inform parents/carers of any incidents of concerns as and when required.

1.4.4 How will e–Safety complaints be handled?

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.

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- 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.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

1.4.5 How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to e–Safety when College resources are being used.
- The school will be sensitive to Internet-related issues experienced by students out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide access to an AUP for any guest who needs to access the school computer system or internet on site.

1.4.6 How will Cyberbullying be managed?

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

It is essential that young people, school staff and parents and carers understand how cyber bullying 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.

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:

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

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

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.

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

The College trains cybermentors under the BeatBullying CyberMentors scheme and actively promotes the resources to all students.

- 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 behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- 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.
- 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.
- Cyberbulling issues need to be dealt with under the standard school behaviour policy

1.4.7 How will Learning Platforms be managed?

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.

The Learning Platform/Environment (LP) must be used subject to careful monitoring bythe 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.

- 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 (if they are enabled)
- Students/staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- Any concerns about content on the LP may be recorded and dealt with in the following ways:

  a) The user will be asked to remove any material deemed to be inappropriate or offensive.
  b) The material will be removed by the site administrator if the user does not comply.
  c) Access to the LP for the user may be suspended.
  d) The user will need to discuss the issues with a member of SLT before reinstatement.
  e) A student’s parent/carer may be informed.

- 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.
- 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.

1.4.8 How will mobile phones and personal devices be managed?

Mobile phones and other personal devices such as Games Consoles, Tablets, PDA , MP3 Players etc. are considered to be an everyday item in today's society and nearly all use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render students or staff subject to cyberbullying;
- Internet access on phones and personal devices can allow students to bypass school security settings and filtering.
- They can undermine classroom discipline as they can be used on "silent" mode;

Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of students or staff.

A policy which prohibits students from taking mobile phones to school could be considered to be unreasonable and unrealistic for schools to achieve. Many parents/carers would also be concerned for health and safety reasons if their child were not allowed to carry a phone and many staff also use mobile phones to stay in touch with family.

Due to the widespread use of personal devices it is essential that schools take steps to ensure mobile phones and devices are used responsibly at school and it is essential that student use of mobile phones does not impede teaching, learning and good order in classrooms. Staff should be given clear boundaries on professional use.

- The use of mobile phones and other personal devices by students and staff in College is permitted for educational activities.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the student or parent/carer.
- If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
- Wireless communication functions, such as Bluetooth, should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such

items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

- Mobile devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.

Student Use of Personal Devices

- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his/her parents/carers they will be allowed to use a school phone. Parents should not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones, devices or accounts for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where telephone contact with student or parents/carers is required.
- Mobile Phones and devices will be switched off or switched to 'silent' mode, wireless communication (such as Bluetooth) switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by their Line Manager.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

1.5 Communication Policy

1.5.1 How will the policy be introduced to students?

Many students are very familiar with 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.

The student and parent agreement form should include a copy of the school e–Safety rules appropriate to the age of the student, as part of the home school agreement

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.

Useful e–Safety programmes include:

Cybermentors: http://www.cybermentors.org.uk/
Think U Know: www.thinkuknow.co.uk
Childnet: www.childnet.com
Kidsmart: www.kidsmart.org.uk
Orange Education: www1.orange.co.uk/education
Safe: www.safesocialnetworking.org

When any user logs into the College network they will automatically be forced to agree to the e-Safety policy. Non-agreement will prevent them from logging in.

- All users will be informed that network and Internet use will be monitored.
- 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.
- Student instruction regarding responsible and safe use will precede Internet access.
- An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- e-Safety rules or copies of the student Acceptable Use Policy will be made public in areas where there is internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where students are considered to be vulnerable.

1.5.2 How will the policy be discussed with staff?

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. 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.

All staff must understand that the rules for information systems misuse for 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.

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.

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.

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and students, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff guidance in safe and responsible Internet use will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- 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.
- 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.

1.5.3 How will parents’ support be enlisted?

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.

- Parents’ attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for students and discuss its implications with their children.

Acknowledgements

Policy constructed by Andrew Field (Head of ICT) and Hillary Hitch (Designated Person for Child Protection) begun in November 2011.

We have used a range of sources and materials including many from the Kent e-Safety officer. Incidentally much of our initial research was carried out by consulting colleagues via Twitter.

Acknowledgements include Rebecca Avery, KCC; Peter Banbury, KCC, Janet Davis, KCC; KCC; Rachel Keen, SENICT; Steve Moores, Maidstone Grammar; Mike O'Connell, CFE Child Protection; Adam Page, EiS; Godfrey Pain, Kent Police; Lindsey Prestage, Libraries, Tracey Tee, Petham Primary; Carol Webb, Invicta Grammar.

Additional people including Kent teachers and officers, SEGfL (South East Grid for Learning), NAACE and the British Computer Society Expert Schools Panel. John Allen, KCC; Steve Bacon, NAACE; Mandy Barrow, Heidi Barton, KCC; Clive Bonner, EiS; Martin Carter, SEGfL; Ian Coulson, KCC; Sandra Crapper, Consultant; Alan Day, KCC Kevin Figg, Westlands; Maureen Gillham, Weald of Kent Grammar; Michael Headley, EiS; Greg Hill, SEGfL; Andrew Lamb, Whitfield Primary; Paul Newton, Kent NGfL; Richard Packham, EiS; Ian Price, Child Protection; Sandra Patrick, Kent NGfL; Tom Phillips, KCC; Graham Read, Simon Langton Girls Grammar; Martin Smith, Highsted Grammar; Chris Shaw, EiS; Linda Shaw, Kent NGfL; Chris Smith, Hong Kong; John Smith, Wakefield LEA; Helen Smith, KCC; Laurie Thomas, Kent; Clare Usher, Hugh Christie; Gita Vyas, Northfleet School for Girls; Ted Wilcox, Borden Grammar. Roger Blamire, BECTA; Stephanie Brivio, Libraries; Les Craggs, KAS; Alastair Fielden, Valence School; John Fulton, Hartsdown; Keith Gillett, Seal Primary; Doreen Hunter, Deanwood Primary Technology School; Steve Murphy, Drapers Mills Primary; Judy Revell, ICT; Chris Ridgeway, Invicta Grammar; Nick Roberts, Sussex LEA; Graham Stabbs, St Margarets at Cliffe Primary; Sharon Sperling, Libraries; Brian Tayler, ICT; Marc Turner, EIS; Joanna Wainwright, KCC; Richard Ward, KCC; Theresa Warford, Libraries; Pam Wemban, Riverview Junior School; Ian Whyte, Plaxtol Primary; Chris Woodley, KCC; Rebecca Wright, KCC; Heather Pettitt, SEGfL; Ian White, SWGfL; Greg Hill, SEGfL.