E-SAFETY POLICY

Policy created:	Policy first adopted:
Signed chair of Governors:	
Re-adopted & signed:	
Consultation:	
E-safety Coordinator June 2014	SLT June 2014
Staff Consultation: 9 June 2014	

1.1 E-SAFETY POLICY IMPLEMENTATION.

The e–Safety Policy and its implementation will be reviewed annually.

Our e–Safety Policy has been written by the college, building on government guidance.

Our College Policy has been agreed by the Senior Leadership Team and approved by governors and other stakeholders. All staff have been involved in the drafting of this policy and consulted about its contents.

The College e-Safety Coordinator is Alan Messer, Lead Teacher for ICT

Contents **page**

1.2 Teaching and Learning

- 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.
- Oak Grove College has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside college and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in college is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the college's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

1.2.1 How does Internet use benefit education?

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 colleges;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of colleges, 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 WSCC and DfE;
- access to learning wherever and whenever convenient.

1.2.2 How can Internet use enhance learning?

Increased computer numbers and improved Internet access may be provided but its impact on pupils' learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils 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 college's Internet access will be designed to enhance and extend education.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- The colleges will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

1.2.3 How will pupils learn how to evaluate Internet content?

- Pupils will be taught at a level appropriate to them, to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils 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-college requirement across the curriculum.

1.3 Managing Information Systems

1.3.1 How will information systems security be maintained?

- The security of the college 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 or password protected
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the college's network will be checked regularly.
- The network manager will review system capacity regularly.
- The use of user logins and passwords to access the college network will be enforced.

1.3.2 How will email be managed?

- Pupils may only use approved email accounts for college purposes.
- Pupils must tell a designated member of staff immediately if they receive offensive email.
- Pupils 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 college provided email accounts to communicate with pupils and parents/carers, in line with professional safeguarding and confidentiality guidelines.
- Access in college to external personal email accounts may be blocked.

- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on college headed paper would be.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during college hours or for professional purposes.

1.3.3 How will published content be managed?

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

1.3.4 Can pupils' images or work be published?

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

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

- The college will control access to social media and social networking sites.
- Pupils 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, college attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with pupils 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 college website with approval from the Senior Leadership Team. Members of staff should not run social network spaces for pupil use on a personal basis.

- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the college where possible.
- Pupils 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. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private. Pupils will be taught about the minimum age for use of different social networking sites.
- All members of the college community should not publish specific private thoughts, especially those that may be considered threatening, hurtful, defamatory and unprofessional or which would identify another person.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of college) 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 college Acceptable Use Policy.

1.3.6 How will filtering be managed?

- The college's broadband access will include filtering appropriate to the age and maturity of pupils.
- The college will work with WSCC and the College's Broadband team to ensure that filtering policy is continually reviewed.
- The college will have a clear procedure for reporting breaches of filtering. All members of the college community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the College e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The college filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the college 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.
- The College Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the college believes is illegal will be reported to appropriate agencies such as IWF, West Sussex Police or CEOP.
- The college's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

1.3.7 How will videoconferencing be managed?

- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the college Website.
- The equipment must be secure and if necessary locked away when not in use.
- College videoconferencing equipment will not be taken off college premises without permission.
- Responsibility for the use of the videoconferencing equipment outside college time will be established with care.

Users

- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents' / carers' consent should be obtained prior to children taking part in videoconferences.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non college site it is important to check that they are delivering material that is appropriate for your class.

1.3.8 How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in college is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the college Acceptable Use Policy.

1.3.9 How should personal data be protected?

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

1.4 Policy Decisions

- The college will maintain a current record of all staff and pupils who are granted access to the college's electronic communications.
- All staff will read and sign the College Acceptable Use Policy before using any college ICT resources.
- Parents will be asked to read the College Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the college site who require access to the college's network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the college community the college will make decisions based on the specific needs and understanding of the pupil(s).
- Students will apply for Internet access individually (if appropriate) by agreeing to comply with the College e-Safety Rules or Acceptable Use Policy.

1.4.1 How will risks be assessed?

The college 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 college computer. Neither the college nor WSCC can accept liability for the material accessed, or any consequences resulting from Internet use.

- The college 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 Sussex Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

1.4.2 How will the college respond to any incidents of concern?

- All members of the college community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the College e-Safety incident log, which is located with the Serious Incident Book in the

Deputy Head teacher's office and other in any relevant areas e.g. Bullying or Child protection log.

- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The college will manage e-Safety incidents in accordance with the college discipline/ behaviour policy where appropriate.
- The college will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the college will debrief, indentify lessons learnt and implement any changes required.
    - Where there is cause for concern or fear that illegal activity has taken place or is taking place then the college will contact the Children's Access Point Officer or the ICT in Schools Officer and escalate the concern to the Police.
    - If the college is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Children's Access Point Officer or the ICT in Schools Officer.
    - If an incident of concern needs to be passed beyond the college then the concern will be escalated to the ICT in Schools Officer.

1.4.3 How will e–Safety complaints be handled?

- Any complaint about staff misuse will be referred to the head teacher.
- All e–Safety complaints and incidents will be recorded by the college, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the college to resolve issues.
- All members of the college community will need to be aware of the importance of confidentiality and the need to follow the official college procedures for reporting concerns.
- Discussions will be held with the Children's Safeguarding Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the college's disciplinary, behaviour and child protection procedures.
- All members of the college 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 college community.

1.4.4 How is the Internet used across the community?

- The college will be sensitive to Internet-related issues experienced by pupils out of college, e.g. social networking sites, and offer appropriate advice.
- The college will provide appropriate levels of supervision for students who use the internet and technology whilst on the college site.
- The college will provide an Acceptable Use Policy (AUP) for any guest who needs to access the college computer system or internet on site.

1.4.5 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.
- Cyberbullying (along with all other forms of bullying) of any member of the college community will not be tolerated. Full details are set out in the college's policy on anti-bullying and behaviour.
- All incidents of cyberbullying reported to the college will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The college will take steps to identify the bully, where possible and appropriate. This may include examining college system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the college to support the approach to cyberbullying and the college's e-Safety ethos.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate.
    - A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at college for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the colleges anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

1.4.6 How will Learning Platforms be managed?

- Staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.

- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.
- When staff, pupils etc. leave the college their account or rights to specific college areas will be disabled or transferred to their new establishment.
- Any concerns about content on the LP may be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - The material will be removed by the site administrator if the user does not comply.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of SLT before reinstatement.
    - A pupil's parent/carer may be informed.

1.4.7 How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by students and staff in college will be decided by the college and covered in the college Acceptable Use or Mobile Phone Policies. College students should not have their mobile phones on them during the college day.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the college community and any breaches will be dealt with as part of the college discipline/behaviour policy.
- College staff may confiscate a phone or device if they believe it is being used to contravene the college's behaviour or bullying policy. The phone or device might be searched by the Senior Leadership Team with the consent of the pupil 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 college time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
- The Bluetooth function of a mobile phone 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 college are the responsibility of the user. The college accepts no responsibility for the loss, theft or damage of such items. Nor will the college accept responsibility for any adverse health effects caused by any such devices either potential or actual.

- Mobile phones and personal devices are not permitted to be used in certain areas within the college site such as changing rooms, toilets and swimming pools.

1.4.8 Pupils' Use of Personal Devices

- If a pupil breaches the college policy then the phone or device will be confiscated and will be held in a secure place in the relevant Head of Year Office. Mobile phones and devices will be released to parents/carers.
- Phones and devices must not be taken into examinations. Pupils 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 pupil needs to contact his/her parents/carers they will be allowed to use a college phone. Parents are advised not to contact their child via their mobile phone during the college day, but to contact College Reception.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

1.4.9 Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Mobile phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or 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 the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the college policy then disciplinary action may be taken.

1.5 Communication Policy

- All users will be informed that network and Internet use will be monitored.
- An e-Safety training programme will be established across the college to raise the awareness and importance of safe and responsible internet use amongst pupils, as part of the ICT provision.
- Pupil instruction regarding responsible and safe use will precede Internet access.

- An e–Safety module will be included in the ICT programmes covering both safe college and home use.
- e–Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- e-Safety rules in an inclusive format will be posted in all rooms with 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 pupils are considered to be vulnerable.

1.5.1 How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the college 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 training in safe and responsible Internet use, both professionally and personally, 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 College 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 pupils.
- All members of staff will be made aware that their online conduct out of college could have an impact on their role and reputation within college. 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.

1.5.2 How will parents' support be enlisted?

- Parents' attention will be drawn to the college e–Safety Policy in newsletters and on the college website.
- A partnership approach to e-Safety at home and at college 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.
- Parents will be requested to sign an e–Safety/Internet agreement as part of the Home College Agreement.
- Parents will be encouraged to read the college Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.

- 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.
- Interested parents will be referred to organisations listed in the "e-Safety Contacts and References section".

Appendix 1

e-Safety Contacts and References

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

Childline: www.childline.org.uk

Childnet: www.childnet.com

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

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

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

West Sussex Police: In an emergency (a life is in danger or a crime in progress) dial 999.

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com