Dartford
SCIENCE & TECHNOLOGY COLLEGE

eSafety and Internet Access Policy

This policy applies to all Internet, Intranet, Nexus, e-mail, messaging systems and all related technology services provided by Dartford Science and Technology College (DSTC).

Aims of the policy

DSTC recognises that the internet and information communication technologies are an important part of everyday life, so students must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

This policy should be read alongside the Safeguarding policy and the Preventing Extremism and Radicalisation policy.

All staff at the College have a duty to ensure that all students and staff are protected from potential harm online.

The purpose of this eSafety policy is to:

- Clearly identify the key principles expected of all members of the College with regards to the safe and responsible use of technology to ensure that DSTC is a safe and secure environment.
- Safeguard and protect all members of the College community online, including prevention of cyber-bullying.
- Raise awareness with all members of the College community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the College.
- Ensuring students are only able to access age appropriate information, images and video material.

Scope of the policy

This policy applies to all anyone who requires usage or access to DSTC’s computer system including the governing body (GB), teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the College (collectively referred to as ‘staff‘ in this policy) as well as students and parents/carers.

This policy applies to all access to the internet and use of information communication devices, including personal devices linked to the College system, or where students, staff or other individuals have been provided with College issued devices for use off-site, such as a work laptops, tablets or mobile phones.

Key responsibilities for the community

The key responsibilities of the e-Safety officer, Senior Leadership Team (SLT) and Governing body are set out below:

- Promoting the online safety vision and culture to all members of the College using government and local authority guidance for support.

- Ensuring that online safety is viewed by everyone in the College as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Child Protection Officer (DCPO) by ensuring they have sufficient resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect students from inappropriate content, whilst still ensuring children have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of College systems and networks and to ensure that the College network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole College curriculum which enables all students to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels that College staff, students and parents can access regarding online safety concerns.
- Ensure that appropriate risk assessments are undertaken regarding the To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

The key responsibilities of the Designated Child Protection Officer (DCPO) are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers including inviting involvement in the annual 'eSafety fortnight.'
- Maintaining a record of online safety concerns/incidents and actions taken as part of the Colleges safeguarding recording structures and mechanisms.
- Monitor the Colleges online safety incidents to identify gaps/trends and use this data to update the Colleges education response to reflect need.
- To report to the Senior Leadership team (SLT), GB and other agencies as appropriate, on online safety concerns.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Meet regularly with the governor with a lead responsibility for online safety as part of the wider safeguarding procedures and reviews.

The key responsibilities for all members of staff are:

- Taking responsibility for the security of College systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the students in their care.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in the curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following the College safeguarding policy.
- Knowing when and how to escalate online safety issues.
- Being able to signpost to appropriate support available for online safety issues.

- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrating an emphasis on positive learning opportunities.

In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with SLT.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on College-owned devices.
- Ensuring that the Colleges filtering policy is applied and updated on a regular basis.
- Ensuring that the use of the College's network is regularly monitored and reporting any deliberate or accidental misuse to the DCPO.
- Report any breaches or concerns to the DCPO and SLT and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DCPO and SLT, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the College's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.

The key responsibilities of children and young people are:

- Contributing to the development of online safety policies where appropriate.
- Reading the College Acceptable Use Policy (which are displayed in classrooms) and adhering to them. See Appendix.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

- **The key responsibilities of parents and carers are:**
- Reading the College Acceptable Use Policy (which are on the College website), encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the College in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the College, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

- Online Communication and Safer Use of Technology
- Managing the College website
- The College will ensure that information posted on the College website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the College address, email and telephone number. Staff or students' personal information will not be published.
- The Principal will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website will comply with the guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.

- The College will post information about safeguarding, including online safety, on the College website for members of the community.

Publishing images and videos online

The College will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media and the safeguarding policy.

All images will be checked against the 'do not photograph list' before publishing online. This list can be found on SIMs.

<u>Managing email</u>

- Students may only use College email accounts for educational purposes
- All members of staff are provided with a specific College email address to use for any official communication.
- The use of personal email addresses by staff for any official College business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email or as attachments with password protection.
- Access to College email systems will always take place in accordance to data protection legislation and in line with other appropriate College policies.
- Members of the staff must immediately tell a member of SLT if they receive offensive communication and this will be recorded in the College safeguarding files/records if appropriate.
- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and students and/or parents.
- Email sent to external organisations should be written carefully, in the same way as a letter written on College headed paper would be.
- The College will have a dedicated email for reporting bullying issues. This inbox is managed by Pastoral Leaders.
- College email addresses and other official contact details will not be used for setting up personal social media accounts.

Use of Social Media
See also Social Media Policy

Expectations regarding safe and responsible use of social media will apply to all members of DSTC community and exist in order to safeguard both the College and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multi-player online gaming, apps, video/photo sharing sites, chat rooms, instant messenger and many others.

- All members of the College will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the College.
- All members of the College are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

- The College will control student access to social media and social networking sites when using College provided devices and systems.

Official use of social media

- Official use of social media sites by the College will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Staff will use College provided email addresses to register for and manage any official approved social media channels.
- Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying and safeguarding policy.
- Public communications on behalf of the College will, where possible, be read and agreed by at least one other colleague.
- Official social media channels will link back to the College website to demonstrate that the account is official.
- The College will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff personal use of social media
See also Social Media Policy and Staff Code of Conduct

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Any communication from students/parents received on personal social media accounts will be reported to the staff members line manager or the DCPO if appropriate.
- Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with Colleges policies and the wider professional and legal framework.
- Members of staff are encouraged not to identify themselves as employees of DSTC on their personal social networking accounts. This is to prevent information on these sites from being linked with the College and also to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as that of the College on social media.
- College email addresses must not be used for setting up personal social media accounts.

Students use of social media

As part of the College’s drive to safeguard students regular advice will be given to students on how to keep safe online. This will be through eSafety events, assemblies, form activities and curriculum activities. The key messages will be:

- Students need to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, College attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Students need to remember not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Students need to understand appropriate security on social media sites and will be encouraged to use safe passwords, deny access to unknown individuals and be supported in learning how to block and report 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/protected.

Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at College, will be dealt with in accordance with existing College policies including anti-bullying and behaviour.

Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at College, will be raised with parents/carers, as appropriate.

Use of Personal Devices and Mobile Phones
See also Behaviour Policy

DSTC recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within the College.

Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The College accepts no responsibility for the loss, theft or damage of such items.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the behaviour policy.

Policy Decisions

DSTC is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

The College will ensure that appropriate filtering and monitoring systems are in place to prevent staff and students from accessing unsuitable or illegal content.

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 always possible to guarantee that access to unsuitable material will never occur via a College computer or device.

The College will audit technology use to establish if the eSafety policy is adequate and that the implementation of the policy is appropriate.

Methods to identify, assess and minimise online risks will be reviewed regularly by the SLT.

Managing Information Systems

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

- The security of the College information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the College's network will be regularly checked for any inappropriate material.
- The network manager will review system capacity regularly.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The College will log and record internet use on all College owned devices.

Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and students must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access College systems. Members of staff are responsible for keeping their password private.

Filtering and Monitoring

- The network manager will support the GB/SLT in ensuring that the College has age and ability appropriate filtering and monitoring in place whilst using College devices and systems to limit children's exposure to online risks.
- All monitoring of College owned/provided systems will take place to safeguard members of the community.
- College systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The College uses educational filtered secure broadband connectivity through the KPSN which is appropriate to the age and requirement of our students.
- The College uses Light Speed filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The College will work with KCC and the Colleges broadband/filtering provider to ensure that filtering policy is continually reviewed.
- The College will have a clear procedure for reporting breaches of filtering which all members of the College community (all staff and all students) will be made aware of. See the safeguarding policy.
- If staff or students discover unsuitable sites, the URL will be reported to the College DCPO and will then be recorded and escalated and blocked as appropriate.
- The College filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- All changes to the College filtering policy will be logged and recorded.
- The network manager will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the College believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately.

Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for students.
- All members of the College community will be informed about the procedure for reporting eSafety concerns, such as breaches of filtering, sexting, cyber bullying, illegal content etc.
- The DCPO will be informed of any e-Safety incidents involving child protection concerns, which will then be recorded.
- The DCPO will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the College's complaints procedure.
- Complaints about online/cyber bullying will be dealt with under the College's anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the Principal
- Any allegations against a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO).
- Staff will be informed of the complaints and whistleblowing procedure.
- The College will manage eSafety 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, identify lessons learnt and implement any changes as 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 Education Safeguards Team or Kent Police.

- If the College is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the College community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in Kent.
- Parents and students will need to work in partnership with the College to resolve issues.

Procedures for Responding to Specific Online Incidents or Concerns
Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

DSTC ensures that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
The College will implement preventative approaches via a range of age and ability appropriate educational approaches for students, staff and parents/carers.

DSTC views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the DCPO.
The College will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in Colleges and colleges: responding to incidents and safeguarding young people' and KSCB "Responding to youth produced sexual imagery" guidance.

If the College is made aware of incident involving creating youth produced sexual imagery the College will:

- Act in accordance with the Colleges child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
- Immediately notify the DCPO.
- Store the device securely.
- Carry out a risk assessment in relation to the student(s) involved.
- Consider the vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Implement appropriate sanctions in accordance with the Colleges behaviour policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the College is implementing best practice and SLT will review and update any management procedures where necessary.
- Inform parents/carers about the incident and how it is being managed.
- If an indecent image has been taken or shared on the Colleges network or devices then the College will take action to block access to all users and isolate the image.
- The College will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Responding to concerns regarding Online Child Sexual Abuse and Exploitation
DSTC will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.

The College will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for students, staff and parents/carers.
DSTC views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the DCPO.

If the College is unclear if a criminal offence has been committed then the DCPO will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

If the College is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the CSET team by the DCPO.

If the College are made aware of incident involving online child sexual abuse of a child then the College will:

- Act in accordance with the Colleges child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
- Immediately notify the designated safeguarding lead.
- Store any devices involved securely.
- Immediately inform Kent police
- Where appropriate the College will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the College is implementing best practice and the College leadership team will review and update any management procedures where necessary.
- The College will take action regarding online child sexual abuse regardless of the use of College equipment or personal equipment, both on and off the College premises.
- The College will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If students at other Colleges are believed to have been targeted then the College will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
- The College will ensure that the Click CEOP report button is visible and available to students and other members of the College community.

Responding to concerns regarding radicalisation and extremism online
See also Preventing Extremism and Radicalisation policy

- The College will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in Colleges and that suitable filtering is in place which takes into account the needs of students.
- When concerns are noted by staff that a student may be at risk of radicalisation online then the DCPO will be informed immediately and action will be taken in line with the safeguarding policy and preventing extremism and radicalisation policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing College policies, including anti-bullying, behaviour etc. If the College is unclear if a criminal offence has been committed then the DCPO will obtain advice immediately via the Education Safeguarding Team and/or Kent Police.

- **Responding to concerns regarding cyber bullying**
- Cyber bullying, 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 policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the College community affected by online bullying.
- Students, staff and parents/carers will be advised to keep a record of cyber bullying as evidence.
- Students, staff and parents/carers will be required to work with the College to support the approach to cyber bullying and the Colleges e-Safety ethos.

:

Internet Access Policy

The Importance of Internet Access at Dartford Science & Technology College

- To raise educational standards.
- To support the professional work of staff.
- To enhance the College's management of information and business administration systems.

Access to the Internet is a necessary tool for staff and an entitlement for students who show a mature and responsible approach. However, the use of the College computer systems either without permission or for purposes not agreed by the senior management could constitute a criminal offence under the Computer Misuse Act 1990.

Benefits of Internet Access

Studies have indicated that benefits gained through appropriate Internet use in education include:

- Access to world-wide educational resources.
- Inclusion in government initiatives.
- Information and cultural exchange between students world-wide.
- News and current events.
- Discussion with experts for students and staff.
- Staff professional development – access to curriculum materials and good practice.
- Communication with advisory and support services, professional associations and colleagues.
- Exchange of curriculum and administrative data with the LEA and DfE.

Risk Assessment

The College recognises that in common with other media such as books, magazines and video, some material available via the Internet is unsuitable for students. The College will supervise students and take all reasonable precautions to ensure that users only access appropriate materials, including having the provided service filtered. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a terminal. Neither the College nor the Co-operative Trust nor KCC can accept liability for the material accessed, or any consequences thereof.

- Regular reviews will take place to quantify and minimise risks.
- Staff, governors, parents and advisors will work together to ensure that every reasonable measure is being taken.
- The Principal will ensure that this policy is implemented effectively.

Authorised Access

- All teaching and support staff will have access to the Internet for professional purposes.
- Internet access can be a necessary part of planned lessons and an entitlement for students based on responsible use.
- An assumption will be made *loco parentis* that parents' permission has been granted for Internet access.
- A record will be maintained by the Network Manager of all staff and students Internet access history.

Security

- Security strategies will be discussed with the LEA.
- The Network Manager will monitor any adverse or anomalous Internet traffic on the College network and will report any problems to the Principal, SLT and Business Manager.
- Virus and Malware protection of the College networks will be updated regularly.
- Students and staff will be advised about security issues in connection with their use of the Internet.
- Any attempt to by-pass the security of the College's web filter is expressly forbidden.

Internet Use for Effective Learning

- Internet access will be planned to enrich and extend learning activities as an integrated part of the curriculum.
- Students will be given clear objectives for Internet use.
- Students will be provided with lists of relevant Web sites.
- Students will be educated in taking responsibility for Internet access.
- Students will be told that random checks will be made on Web sites accessed.
- Students using the Internet will be supervised appropriately.
- Internet access will be purchased from a supplier that provides a service designed for students which includes appropriate filtering.
- The College will work with the LEA and the Internet provider to ensure that systems to protect students are regularly reviewed and improved.

Student Assessment of Internet Content

- Students will be taught that they should validate information obtained via the Internet.
- Students will be taught to observe copyright when copying materials from the Web.
- Students will be taught the problems associated with the internet via e-safety training as part of the College's eSafety fortnight.
- Students will be taught that the Web provides a wider range and level of content than College libraries or TV.
- Students will be expected to report any unsuitable material they encounter during genuine research on the Web.

E-mail

- Students are expected to use e-mail.
- E-mail communications will be managed to ensure appropriate educational use and that the good name of the College is maintained.
- The forwarding of chain letters via e-mail is forbidden.
- Incoming e-mail received via the network will be randomly checked by the Network Manager to ensure appropriate safeguarding measures are in place.
- Students in all year groups will have e-mail accounts.
- E-mail accounts will be provided for teaching and support staff.
- All emails will contain an approved disclaimer.

The College Web Site

- The College will maintain and update the existing Web site with editorial responsibility being delegated to a member of staff who will ensure accuracy of content and quality of presentation.
- Students' work may be published on the College site if this is appropriate and it complies with the above.
- The point of contact on the College's Web site must be the College address, a default email address and telephone number – students' private home addresses or telephone numbers must not be published.
- Published images and text must not contain any identifiable matter that relates to a student.

- Students' images that have, "Do Not Photograph" ticked with the College's Management Information System must not be used at all.

Remote Access

- Remote access to the College's network is available via 'Nexus'
- During the course of using Nexus teachers are functioning as employees of the College and will follow the same agreed procedures as if they were on site.

Appropriate Access

- Staff will check suggested Web sites are appropriate to the age and maturity of the students.
- Student access levels will be regularly reviewed in the light of experience of use.
- All staff using the Internet with students will make regular checks on Internet sites visited to monitor compliance with the College Internet Access Policy.

Complaints

- Responsibility for handling incidents of misuse of the College computer systems will be given to the pastoral lead.
- Students and parents will be informed of action to be taken in the event of misuse of the computer systems.
- If staff or students discover unsuitable sites the URL (address) and content will be reported to the Internet Service Provider.
- Any material that the College suspects is illegal will be referred to the police.
- Sanctions for misuse of the College computer systems will be in line with the College discipline policy, and may include having some access rights withdrawn.

Information about Internet Access and Responsibility

- The College Internet Access Policy will be included in the staff handbook.
- All teaching and non-teaching staff, and parents of College students will be made aware of the policy and its importance.
- All students will receive training on responsible Internet use during their ICT lessons and as part of the College's Safety fortnight. Rules for Internet access will be posted in all rooms in the College which have computers. See appendix.

Appendix – Rules displayed in College classrooms with computers

The computer systems are owned by the College. They may be used by students to further their education and by staff to enhance their professional activities in connection with the College. The College Internet Access Policy has been drawn up to protect students, staff and parents.

The College reserves the right to examine or delete any files that may be held on its computer system, or to monitor any Internet sites visited.

- All Internet activity should be appropriate to staff professional activity or the students' education.
- Access should be made via the user's own password which should not be made available to any other person.
- Any activity that may cause damage or failure to the College ICT systems, or to other systems, is forbidden.
- Copyright of materials must be respected.
- E-mail forwarded on College business must use the same professional levels of language and content as for letter and other media sent by the College.
- Posting anonymous messages or forwarding chain letters is forbidden.
- Use of the network to access inappropriate materials is forbidden.