Multi Academy Trust

Online Safety Policy

White Cliffs Primary College for the Arts

Policy reviewed and ratified:	16 January 2017
Policy review date:	31 January 2019

At White Cliffs Primary College for the Arts we believe that the use of computers and information and communication technologies brings great benefits. Recognising the Online

Safety issues and planning accordingly ensures the appropriate, effective and safer use of electronic communications.

Who will write and review the policy?

The Online Safety Policy is part of the ICT Computing and Safeguarding Policies. It relates to other policies including those for Behaviour, Anti-bullying, Personal, Social and Health Education (PSHE) and Learning for Life.

The Vice Principal, is the member of the Leadership Team responsible for Online Safety.
Our Online Safety Policy has been written by the College, building on the KCC Online Safety Policy and government guidance. It has been agreed by the College Leadership Team and approved by Board of Directors.

The Vice Principal is also the Designated Child Safeguarding Lead with specific responsibility for Online Safety.

Teaching and Learning

Why is Internet use important?

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction. The College has a duty to provide pupils 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 pupils who show a responsible approach to its use.

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 pupil attainment.

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries.
- 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 KCC and DFE.
- Access to learning wherever and whenever convenient.

How can Internet use enhance learning?

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 are being 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 College will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes appropriate for the age of the pupil.
- 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.

How will pupils 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.

- Pupils should be taught 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, overseen by a member of staff.
- The evaluation of online materials is a part of teaching/learning in every subject.

Managing Information Systems

How will information systems security be maintained?

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

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.
- For College staff, flouting electronic use policy is regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Workstations should be secured against user mistakes and deliberate actions. Workstations should be "locked" or shut down when not in use.
- 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. Wide Area Network (WAN) security issues include:
- All Internet connections must be arranged via the EIS Broadband team to ensure compliance with the security policy.
- EIS Broadband firewalls and EIS are configured to prevent unauthorised access between Colleges.
- Decisions on WAN security are made on a partnership basis between Colleges and KCC/EIS.

The College's Broadband network includes a cluster of high performance firewalls at each of the Internet connecting nodes. These appliances run industry leading software and are monitored and maintained by a specialist security command centre.

- The security of the College information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the College's network will be regularly checked.
- The Network Manager will review system capacity regularly.

How will email be managed?

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

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

- Whole class or group email addresses will be used in primary Colleges for communication outside of the College.
- Access in College to external personal email accounts may be blocked.
- College email addressed should not be used in a social context.
- 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.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during College hours or for professional purposes.

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 Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the College's guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?

Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount.

Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown.

- Images 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 or when forwarding images to third party (where permission from parents and carers has been granted), particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published, or passed on to third parties for publication (e.g. newspapers).
- Pupils' work can only be published with the permission of the parents.

Managing the use of pupil images;

- Pupil's images that are used to record activities and external visits outside of the College must only be taken with approved College equipment - use of personal recording equipment such as mobile phones is prohibited.
- Images are to be stored securely on the College's network or on College equipment such as cameras or tablet computers. Where equipment is portable, it must be password protected wherever possible and equipment should be kept in locked storage when not in use.
- Permission for use of such images for recording and evaluating purposes must be approved by the parent/carer upon joining the College.
- The sharing of images is strictly prohibited in all other contexts, with the exception of website/newspaper publication in line with the permission letter signed by parents/carers upon their child's enrolment at the College.

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

- The College will control access to social media and social networking sites.
- Pupils, parents and carers will be informed as to the suitability of particular sites, and actively encouraged to use age-appropriate sites only. They will also be advised to keep any social networking access secure.
- Parents and carers will be advised to monitor their child's use of social media and messaging platforms outside of College.
- 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.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the student or his/her location.
- Staff are not permitted to make reference to pupils on their own personal social networking sites.
- If personal publishing is to be used with pupils then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by College staff.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

How will filtering be managed?

- The College will work with KCC, EIS and the College's Broadband team to ensure that systems to protect pupils are reviewed and improved.

- If staff or pupils discover unsuitable sites, the URL must be reported to the Director/DSL for Online Safety or the Network Manager.
- The College's broadband access will include filtering appropriate to the age and maturity of pupils.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any issues or concerns are reported to the CEO via the Principal and addressed with the Federation Leadership Team.
- Any material that the College believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

How will video conferencing be managed?

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Video conferencing contact information should not be put on the College Website.
- The equipment must be secure and if necessary locked away when not in use.
- College video conferencing equipment should not be taken off College premises without permission.

Users:

- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing should be supervised appropriately for the pupils' age.
- Parents and carers should agree for their children to take part in video conferences.
- Only key administrators should be given access to video conferencing administration areas or remote control pages.
- Unique log on and password details for the educational video conferencing services should only be issued to members of staff and kept secure.

Content:

- When recording a video conference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of video conference should be clear to all parties at the start of the conference.
- Recorded material shall be stored securely.
- Video conferencing 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 video conference. If it is a non-College site it is important to check that they are delivering material that is appropriate for your class.

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in College is allowed.

How will the use of mobile phones be managed?

- Staff will be issued with a College phone where contact with pupils is required, or when there is a need for a member of staff to be in contact with College or parents (e.g. school trip).
- Mobile phones will not be used by pupils anywhere on the College site for any purpose, including making calls, accessing internet or games, recording sound/video or taking photos. Where a child has a mobile phone provided by a parent/carer for security when walking to or from the College, it must be handed in to the office and labelled with the child's full name and class.
- Staff should not use any personal equipment such as mobile phones or cameras for College purposes. Under no circumstances should images be recorded on equipment other than that provided by College for that express purpose.
- Personal mobile phones should not be used by staff in classrooms or any areas where children may be present at any time.

How should personal data be protected?

The quantity and variety of data held on pupils, 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 ie subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully.

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

Policy Decisions

How will Internet access be authorised?

- The College will maintain a current record of all staff and pupils who are granted access to the College's electronic communications.
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any College ICT resource.
- All pupils will be introduced to the College rules of safe use of the Internet and agree to abide by them.
- Parents will be asked to sign and return a consent form for pupil access.

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 KCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The College should audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online 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.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will Online Safety complaints be handled?

- Complaints of Internet misuse will be dealt with under the Grievance and Complaints Procedure.
- Any complaint about staff misuse must be referred to the Principal.
- All Online 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 work in partnership with staff to resolve issues.
- Any issues (including sanctions) will be dealt with according to the College's disciplinary and child protection procedures.

How is the Internet used across the community?

- The College will liaise with local organisations to establish a common approach to Online Safety.
- 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 work in partnership with parents and carers to advise them on Online Safety concerns. In the event that an incident that has occurred outside of the College is reported on to staff, parents/carers of the pupils involved in the incident will be informed.
- Consultation and/or referral to Children's' Social Services will be made if there is any potential safeguarding issue relating to Online Safety concerns outside of College, in accordance with the KCC/Kent Police "Response to an Incident of Concern" document (see appendix).

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.

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

- Cyberbullying (along with all forms of bullying) will not be tolerated in College. Full details are set out in the College's policy on anti-bullying.
- All incidents of cyberbullying reported to the College will be recorded.
- Clear procedures are in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers are advised to keep a record of the bullying as evidence.
- The College will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content.
    - Internet access may be suspended at College for the user for a period of time.
    - Parents/carers may be informed.
    - The Police will be contacted if a criminal offence is suspected.

How will Learning Platforms and learning environments be managed?

An effective learning environment can offer Colleges a wide range of benefits to teachers, pupils, parents as well as support management and administration. It can enable pupils and teachers to collaborate in and across Colleges, can share resources and tools for a range of topics, create and manage digital content and pupils can develop online and secure e-portfolios. Examples of learning environments used at the College include "Lexia", Symphony Maths" and "Accelerated reader."

- The College Leadership Team and staff will monitor usage by pupils and staff regularly in all areas.
- Permission must be sought from a pupil's parent or carer before that pupil may use any Learning platform or environment.
- Pupils/staff will be advised on acceptable conduct and use when using the learning environment.
- When staff, pupils etc. leave the College their account or rights to specific College areas will be disabled.

Any concerns with content may be recorded and dealt with in the following ways:

- The user will be told 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 for the user may be suspended.
- The user will need to discuss the issues with a member of CLT before reinstatement.
- A pupil's parent/carer may be informed.

Communication Policy

How will the policy be introduced to pupils?

- All users will be informed that network and Internet use will be monitored.
- An on-going Online Safety training programme will raise the awareness and importance of safe and responsible internet use.
- Pupil instruction in responsible and safe use will precede Internet access.
- An Online Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe College and home use.
- Online Safety training will be part of the transition programme into each year group within the College as a refresher for Internet safety rules.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

- The Online 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 should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will be informed to report all Online Safety issues to the College's designated Online Safety Officer.
- Staff that manage filtering systems or monitor ICT use will be supervised by the College Leadership Team and have clear procedures for reporting issues.

How will parents' support be enlisted?

- Parents' attention will be drawn to the College Online Safety Policy in newsletters, the College brochure and on the College website.
- Parents will be requested to sign an e–Safety/internet agreement when a child joins the College, along with giving permission for the use of photographs in different contexts and use of Learning platforms/environments.
- Information and guidance for parents on Online Safety will be made available to parents in a variety of formats and "awareness" communications will be sent home once a year to maintain the profile of Online Safety.

Appendices

1.1 "Response to Incident of Concern" Flowchart

1.2 Online Safety Incident Log

1.3 Staff Code of Conduct for ICT

Appendix 1.1

Schools Designated Safeguarding Leads:

- Mrs S Fotheringham (Principal)
- Mr S Paget (Vice Principal & Online Safety Officer)
- Miss S Kemp (Director of Parent Support)
- Mrs H Castle (Director for Inclusion and Key Stage 1)
- Mr D Stafford (Director of Key Stage 2)
- Miss S Lowe (Director of Early Years)

Response to an Incident of Concern

Contacts

- **Children Safeguard's Unit (CSU)**
  01622 696366
  and speak to a local Children's Officer
- **e-Safety officer:**
  esafetyofficer@kent.gov.uk
  01622 221469
- **Kent Police:**
  01622 690690 (Switch board)
  ask to speak to the Public Protection Unit for your area and/or your Safer School Partnership Coordinator
- **Child Exploitation and Online Protection Centre (CEOP)**
  www.ceop.police.uk

e-Safety incident occurs

If a child is at immediate risk
- Inform the Designated Child Protection Coordinator and follow schools' child protection procedures
- Consult with Children's Safeguarding Unit (CSU)
- Contact Kent Police (999) urgently if there is immediate danger

Illegal Activity or Material found or suspected

Content
- Contact CSU or e-Safety Officer
- Report to Internet Watch Foundation (www.iwf.org.uk) and/or Kent Police

Activity

Child
- Contact CSU and/or e-Safety Officer
- Report to CEOP www.ceop.police.uk
- Child protection procedures and/or criminal action

Staff
- Contact CSU and/or e-Safety Officer
- Staff allegations procedures and/or criminal action

Unsure
- Consult with CSU or e-Safety Officer

Inappropriate Activity or Material

Activity

Child

Possible School Actions:
- Sanctions
- PSHE/citizenship
- Restorative justice
- Anti-bullying
- Parental work
- School support e.g. counselling, peer mentoring
- Request support/advice from e-Safety officer

Staff

Possible School Actions:
- Staff training
- Disciplinary action
- School support e.g. counselling
- Request support/advice from e-Safety Officer

Content
- Report to filtering manager and/or Schools Broadband helpdesk

Review Schools e-Safety policies and procedures, record actions in e-Safety Incident log and implement any changes for the future

Local Contact Details

Schools Designated Child Protection Coordinator:
School e-Safety Coordinator:
e-Safety/Child Protection Governor(s):
Safer School Partnership Coordinator:
Local Children's Officer:
Other useful details:

Kent County Council

Kent Police

Appendix 1.2

Online Safety Incident Log

This is a CONFIDENTIAL DOCUMENT - only use the names of children directly affected by the incident.

- **All safeguarding issues relating to Online Safety incidents must be passed on to one of the College's Designated Child Protection Officers.**
- **Any issues considered to be of a safeguarding matter should be reported on following standard College procedures (i.e. Green Form to Director of Pupil and Parent Support.)**
- **A brief outline of action needs to be given below, along with any outside agencies that have been involved in any investigation.**
- **<u>Remember</u>: Where Online Safety issues occur outside of College, parents must be informed and Children's Social Services must be consulted if there are safeguarding concerns.**

Date	Nature of incident and actions taken:

Appendix 1.3

The Dover Federation for the Arts Multi Academy Trust

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's Online Safety Policy for further information and clarification.

- I understand that it is a criminal offence to use a College/School ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs (Personal Digital Assistant), digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for College/School business.
- I understand that College/School information systems may not be used for private purposes without specific permission from the Principal of each College/School.
- I understand that my use of College/School information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in College/School, taken off the College/School premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Online Safety Coordinator, the Designated Child Protection Coordinator or Principal of College/School.
- I will ensure that electronic communications with pupils including email, IM (Instant Messaging) and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote Online Safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The college/school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the College's/School's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Full Name: ……..