



ESAFETY POLICY

Policy written	July 2010
Staff Responsible:	S. Minhas (Deputy Head Teacher - Standards)
Initial discussion with Governors	July 2010
Approval of policy by Governors	September 2010
Review Date:	September 2011

Contents

- Introduction
- Roles and Responsibilities
- ESafety in the Curriculum
- Password Security
- Data Security
- Managing the Internet Safely
- Managing other Web 2 Technologies
- Mobile Technologies
- Managing Email
- Safe Use of Images Guidelines
- Safe Use of Images Acceptable Use Agreement: Staff, Governors and Visitors
- Safe Use of Images Acceptable Use Agreement: Parents
- Misuse and Infringements
- Equal Opportunities
- Parental Involvement
- Writing and Reviewing this Policy
- ICT and the Related Technologies Acceptable Use Agreement: Staff, Governors and Visitors
- Acceptable Use Agreement: Students
- Flowcharts for Managing an ESafety Incident
- Incident Log
- Displaying ESafety Advice
- Current Legislation
- Data Processor Agreements
- ESafety Audit

Introduction

ICT in the 21st Century is seen as an essential resource to support independent learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Coppice needs to develop the use of these technologies in order to arm our students with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Although ICT is exciting and beneficial both in and out of the context of education, we must recognise that particularly web-based resources; are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Coppice Performing Arts School, we understand the responsibility to educate our students on ESafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy and the Acceptable Use Agreement (for all staff, students, governors and visitors) are inclusive of both fixed and mobile internet; technologies provided by the school - PCs, laptops, Personal Digital Assistants, tablets, whiteboards, digital video equipment, etc; and technologies owned by students and staff, but brought onto school premises -laptops, mobile phones, camera phones, PDAs and portable media players, etc.

Roles and Responsibilities

Senior Management and Governors are regularly updated by the Headteacher and all Governors have an understanding with regard to the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, students, governors and visitors, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour/student discipline, including the anti-bullying policy.

ESafety skills development for staff

- Our staff will receive regular information and training on ESafety issues in the form of In Service Training [INSET] and circulars.
- New staff will receive information on the school's acceptable use policy as part of an induction programme.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of ESafety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)
- Staff where necessary and appropriate incorporate ESafety activities and awareness within their Curriculum Areas.

Managing the school ESafety messages

- We endeavour to embed ESafety messages across the curriculum whenever the internet and/or related technologies are used.
- The ESafety policy will be introduced to the students at the start of each school year.
- ESafety posters will be prominently displayed.
- Upon logging in to the school's computer network, users are expected to read and accept the terms of the A.U.P. Failure to accept the terms of the A.U.P will result in automatic log off from the network.

ESafety in the Curriculum

- The School has a framework for teaching internet skills in ICT lessons.

These are integrated into Key Stage 3 curriculum:

- Year 8 - unit of study with a particular focus on E-Safety.
- Year 9 - revisit to E-Safety issues.

These are integrated into the Key Stage 4 curriculum:

- *OCR Nationals Unit 1, 2, 3, 5, 6 & 7 (for those students opting to follow this course).*
- *Functional ICT, Levels 1 & 2 (only for diploma students at present).*

- Educating students on the dangers of technologies that maybe encountered outside school is done when opportunities arise and as part of the ESafety curriculum.
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Students are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities.
- Students are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent, carer, teacher, trusted staff member, or an organisation such as Childline/CEOP report abuse button.
- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

These are integrated into Key Stage 3 curriculum: *Mapping to the curriculum information to be provided.*

Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's ESafety Policy.
- At regular intervals all users are asked to re-confirm that they have read, understood and accept AUP as they log on. If they do not accept, they are not allowed to continue.
- Users are provided with an individual network, email and Learning Platform log-in username. All students are expected to use a personal password and keep it private.
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If your password may have been compromised or someone else has become aware of your password report this to ICT technical support.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that work stations are not left unattended and are locked.
- Due consideration should be given when logging into the Learning Platform to the browser/cache/cookie options (shared or private computer).
- At Coppice, all ICT password policies are the responsibility of ICT technical support and all staff and students are expected to comply with the policies at all times.

Data Security

The accessing of school data is something that the school takes very seriously. The school follows Becta guidelines (published Autumn 2008)

- Staff are made aware of their responsibility when accessing school data. They must not:
 - allow others to view the data
 - edit the personal data of a student held on the School Information Management System (unless this is part of their specific job description)
 - remove sensitive or personal data from the school premises in electronic form unless the media is encrypted and transported safely
 - store data on an unsecured memory stick or the unencrypted hard drive of a laptop
 - retain personal or sensitive data for longer than required
 - send sensitive personal data via email unless it is from secure site to secure site

They must:

- ensure all personal information is securely destroyed (paper data is shredded and electronic data is over written several times)
- ensure that where personal information is held on paper it is locked away when not in use or the office/desk is secure (i.e. locked when not occupied)

Managing the Internet Safely

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Wolverhampton Grid for Learning (WGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school maintains students will have supervised access (6th Form study room is unsupervised) to internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents re-check these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources. Students will also reference any secondary or intellectual source within their work.

Infrastructure

- Coppice monitors internet use and searches on the network through Cachepilot supplied by Wolverhampton LA.
- Staff and students are aware that school based email and internet activity can be monitored and explored further if required.
- The school uses management control tools (RM tutor and RM Management Console) for controlling and monitoring workstations.
- If staff or students discover an unsuitable site it must be reported to the ICT technical support as soon as possible.
- The school will provide antivirus software on portable computers and the staff member who it is assigned to will have the responsibility of updating the virus definitions.
- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from ICT technical support.
- Wolverhampton LA supplies Kaspersky Internet Security.

Managing other Web 2 Technologies

Web 2/Social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking sites to students and staff within school.
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/home phone numbers, school details, email address, specific hobbies/interests).
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Students and staff are asked to report any incidents of bullying to the school.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using the Coppice Virtual Learning Environment [VLE] Platform or other systems approved by the Headteacher.
- Staff are prohibited from communicating or adding students still listed on roll as "friends" on any social networking platform, Instant messaging program or games service provider. Ex students can only be added at the member of staff's discretion and the understanding that others can access your personal site through them. However it is recommended that no ex students of Coppice Performing Arts School are added.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. The school strongly recommends that staff do not contact a student or parent/carer using their personal device.
- The school would prefer students not to bring personal mobile devices/phones to school. If a student chooses to bring a mobile device to school it must not be used for personal purposes within lesson time. At all times the device must be switched off.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Managing Email

The use of email within most schools is an essential means of communication for both staff and students. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an email in relation to their age and good network etiquette (netiquette). In order to achieve ICT level 4 or above, students must have experienced sending and receiving emails.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that,

"This message contains information that may be privileged or confidential. It is intended only for whom it is addressed. If you are not the intended recipient, you are not authorised to read, print, retain, copy, disseminate, distribute or use this message or any part thereof. If you receive this message in error please notify the sender immediately and delete all copies of this message."

As Internet communications are not secure, please be aware that Coppice cannot accept responsibility for its contents. It is, therefore, your responsibility to scan attachments (if any) for viruses. Any views or opinions presented are those of the author only and not of Coppice. Coppice reserve the right to intercept incoming and outgoing email communications."

- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails from their school account to parents or students are requested to cc. the Headteacher, Line Manager or Head of House
- Students may only use school approved accounts on the school system. The accounts are restricted and can only send and receive emails from email accounts within Coppice or Wolverhampton LA.
- In cases where staff need email contact with students, for example OCR Nationals Unit 1, A02, parents should be notified before hand. A separate email account should be set up as a handing in point. It is advisable for the password to this account to be known by the Network Manager/Headteacher so that messages remain open for scrutiny at all times.

- The forwarding of chain letters is not permitted in school. However the school has set up a dummy account to allow students to forward any chain letters causing them anxiety.
- All email users are expected to adhere to the generally accepted rules of network etiquette, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication.
- Students must immediately tell a teacher/trusted adult if they receive an offensive email.
- Staff must inform technical support if they receive an offensive e-mail or emails that can be considered as Spam.
- Users are sometimes asked to accept this policy as part of the logging on process. If students or staff; refuse to accept they are automatically logged off.

Safe Use of Images

Coppice Performing Arts School

Safeguarding

Staff/Governors/Visitors

Guidelines for safe use of images of students

Please read carefully

Taking of Images and Film

- ✓ With the written consent of parents/carers (on behalf of students) and Staff, Governors and Visitors, the school permits the appropriate taking of images by staff and students with school equipment.
- ✓ Staff/Governors/Visitors/Students are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, including when on field trips or enrichment days, without the express permission of the Headteacher. When permission has been given, images taken must then be transferred immediately and solely to the schools network and deleted from the portable device.

Publishing Students' Images and Work

Parents/Carers will be asked to give their consent for images of their children to be recorded and displayed, including photographs, in the following ways:

- Coppice School website, the prospectus, newsletter, screens, curriculum documents and local press releases. The photographs used will show School Visits, Trips, Enrichment Days, student success/celebration e.g. Year 11 Prom, celebration assemblies, sport team presentations, examination results day, charity events and so on
- Displays within the school
- External exhibitions

This Consent Form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. E.g. Divorce, taken into care

Storage of Images

- When permission has been given to Staff/Governors/Visitors or Students to use personal digital equipment, such as mobile phones and cameras, to record images of students, including when on field trips or enrichment days, images taken must then be transferred immediately and solely to the school's network and deleted from the portable device.
- Images/films of students are stored on the staff area of the school's network only.
- Staff/Governors/Visitors and Students are not permitted to use portable media for storage of images e.g. USB sticks, without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network.
- ICT technical support has the responsibility of deleting the images when they are no longer required, or the student has left the school.

CCTV and Webcams

- The school uses CCTV for security and safety. The only people with access to this are The Headteacher, Site Manager and Caretaker. Notification of CCTV use is displayed around the school.

Coppice Performing Arts School

Safeguarding

Staff/Governors/Visitors' Consent Form

Please read carefully

Use of Photographs, Video or Web

As part of our Safeguarding Procedures we are attempting to make everyone connected with the school aware of our procedures regarding the use of photographs, video or web information related to them.

We use photographs or digital film in school for a number of reasons. The main purpose is to celebrate success, achievement and any interesting or unusual events that take place - the photos are used on display boards, on screens, on the website and occasionally in the local press or media.

We may also use film as a learning tool. For example, acting out scenes in Drama and then playing it back so that the teacher, the student and the class can analyse technique. Or, for example, in an interview situation, if this is relevant to a subject or piece of coursework. In most cases the film is only used within school, but there may be cases where we use materials for public display and/or moderation i.e. Media Studies.

Please note your name will normally be displayed alongside the photograph taken of you if it is of a small group or of an individual.

Coppice School therefore asks for your consent to using material, including photographs of you, in the following ways:

- Coppice School website, the prospectus, newsletter, screens, curriculum documents and local press releases. The photographs used will show School Visits, Trips, Enrichment Days, success/celebration e.g. Year 11 Prom, celebration assemblies, sport team presentations, examination results day, charity events and so on
- Displays within the school
- External exhibitions/Press articles e.g. Express & Star

If you need clarification or are concerned about the use of your photograph please contact Mrs A Cunningham, Headteacher's PA, at school.

CONSENT FORM FOR COMPLETION BY STAFF/GOVERNORS/VISITORS

Please complete this section and return your signed Consent Form to Main Reception

I **agree** to my photograph being used as described above, please tick

I **do not agree** to my photograph being used as outlined above, please tick

This Consent Form is considered valid for the entire period that you attend this school.

You do have the right to withdraw consent at any time by writing to the Headteacher.

Staff/Governor/Visitor Name _____

Signed _____ (Staff/Governor/Visitor)

Date _____

Coppice Performing Arts School

Safeguarding

Parental Consent Form – please read carefully

Use of Photographs, Video or Web

We use photographs or digital film in school for a number of reasons. The main purpose is to celebrate the success of students – the photos are used on display boards, on the plasma screens, on the website and occasionally in the local press or media. Examples include photographs of sports teams, members of the cast of school productions, extra curricular activities, charity events and examination successes.

We may also use film as a Learning tool. For example, acting out scenes in Drama and then playing it back so that the teacher, the student and the class can analyse technique. In most cases the film is only used within school, but there may be cases where we use materials for public display and/or moderation.

Please note your child's name will normally be displayed alongside the photograph if it is of a small group or just of your child.

Coppice School therefore asks for your consent to using material, including photographs, in the following ways:

- Coppice School website, the prospectus, newsletter, screens, curriculum documents and local press releases. The photographs used will show School Visits, Trips, Enrichment Days, student success/celebration e.g. Year 11 Prom, celebration assemblies, sport team presentations, examination results day, charity events and so on
- Displays within the school
- External exhibitions/Press articles e.g. Express & Star

If you need clarification or are concerned about the use of your child's photograph please contact Mrs J Nixon at school.

Students' photographs are also used on our Management Information System which is only accessed by staff. They may also be used for emergency medical notes and by the emergency services in exceptional circumstances.

This section to be completed by Parent/Carer and returned to your child's Academic Tutor

I **agree** to my child's photograph being used as described above, please tick

I **do not agree** to my child's photograph being used as outlined above, please tick

This Consent Form is considered valid for the entire period that your child attends this school unless there is a change in the child's circumstances where consent could be an issue.

Parents/Carers do have the right to withdraw consent at any time by writing to the Headteacher.

Name of child _____ Tutor Group _____

Signed _____ (Parent/Carer)

Date _____

If this form is not returned we regret that we will be unable to include your child in any educational/celebratory photographs

Misuse and Infringements

Complaints

Complaints relating to ESafety should be made to the Headteacher. Incidents should be logged and the Flowcharts for Managing an ESafety Incident should be followed.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher or Deputy Headteacher for Standards.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Headteacher, depending on the seriousness of the offence; investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart on page 28 of this document).
- Users are made aware of sanctions relating to the misuse or misconduct of IT equipment. Staff will all receive a full copy of the ESafety policy and appropriate training and guidance. Governors, Parents, Students and visitors will all sign up to the User Acceptance Policy and where necessary, receive appropriate training and guidance.

Equal Opportunities

Students with additional needs

The school endeavours to create a consistent message with parents and carers for all students and this in turn should aid establishment and future development of the schools' ESafety rules.

Staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of ESafety issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of ESafety. Internet activities are planned and well managed for these children and young people and expectations are clearly explained.

Some students have the opportunity to further enhance their understanding of E-Safety through training provided by Wolverhampton City Learning Centre on an annual basis. Vulnerable students are selected where possible.

Parental Involvement

- Parents/Carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on school website, newsletter, on the School Information Management System)
- The school disseminates information to parents relating to ESafety where appropriate in the form of:
 - Information and celebration evenings
 - Website/ Learning Platform postings
 - Newsletter
 - Guide for Parents
 - School Planner
 - Prospectus

Writing and Reviewing this Policy

Review Procedure

There will be an ongoing opportunity for staff to discuss with the Headteacher any issue of ESafety that concerns them.

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended and approved by the staff, Headteacher and Governors.

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor Acceptable Use Agreement/Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the ESafety coordinator, a member of the Leadership team.

- I will only use the school's email/Internet/Intranet/Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to students.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission of the safety coordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carers, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help students to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature _____ Date _____

Full Name _____ (Printed)

Job title _____

Dear Parent/ Carer

Use of the Internet by Students

As part of the Government drive to personalise learning and to support Learning opportunities within the school, your child, will at appropriate times, be given access to the Internet as an information source, a communications tool and a publishing medium.

The Internet has become a major source of educationally useful material and the primary distribution medium for a wide range of organisations. The potential to support the classroom teacher is significant and will continue to grow.

There are well-publicised concerns regarding access to material on the Internet that would be considered unsuitable for school students. Whilst it is impossible to ensure that a student will not access such material, the school, in liaison with Wolverhampton LA and Research Machines plc, is taking all reasonable steps to minimise a student's access to unsuitable material.

These include:

- Use of filtered Internet Service to prevent access to Internet sites with certain types of material e.g. Pornography, violent, offensive and abusive material.
- Restricted access to 'chat rooms'
- The requirement that wherever possible all Internet access during school hours, for Years 7 - 11, will be supervised by a member of staff or other responsible adult.
- Tracking mechanisms that enable the school to identify which Internet sites have been visited and to monitor Internet access.
- Education of students as to the potential legal consequences of accessing types of material.

Attached to this letter is a copy of the school's Acceptable Use Policy. All users of school equipment are expected to abide by this policy. Users not abiding by this policy may have their right to use the systems withdrawn. For serious offences, the Police or other authorities may have to be informed.

The school's policy on the use of computers and other technologies, including the use of the Internet is available for parents to inspect.

If you would like to discuss any issues surrounding the use of the Internet or the content of this letter please contact the school and ask to speak to me in the first instance.

Yours sincerely

J. Fletcher
Headteacher

Acceptable Use Agreement: Students

Coppice Performing Arts School

Student Acceptable Use Agreement/ESafety Rules

All Activity should be appropriate to the pupil's education as outlined below:

- ✓ All computers, whether desktop machines or laptops belong to the school and all, hardware or software that accompanies them must **NOT** be removed, tampered with or edited in any way.
- ✓ The installation of personal software that has not been done by the system administrator onto a school computer for whatever reason is strictly prohibited for both staff and students.
- ✓ The user assumes full responsibility for any laptop computers and the user **WILL** be held responsible for any, loss, damage or theft on school machines on or off school premises.
- ✓ Access to the Network should only be made via an authorised account and password, which should **NOT** be made available to any other persons.
- ✓ All laptops that are taken off school premises must be connected to the school network at least once a week to cater for network updates.
- ✓ When using a school computer or laptop must be treated with care and respect and must **NOT** be damaged or misused.
- ✓ Students should only use the Internet when given permission to do so by their teacher.
- ✓ Unauthorised access i.e. 'Hacking' or misuse of personal information, contrary to the provision of the Data Protection Act 1988, is a serious offence and is not permitted under any circumstances.
- ✓ Intentional damage to a computer or the computer network, including unauthorised damage or interference to any files, may be considered a criminal offence under the Computer Misuse Act 1990
- ✓ Any unauthorised copying of software contrary to the provisions of the Copyright, Designs & Patents Act 1988 is not permitted.
- ✓ The downloading and saving of MP3 music files is strictly prohibited
- ✓ Users are responsible for all e-mail sent and for contacts to be made that may result in e-mail being received.
- ✓ Use for personal financial gain, gambling political purposes or advertising is forbidden

- ✓ Posting anonymous messages, forwarding chain letters and causing others to receive unwanted messages or goods are forbidden.
- ✓ Using the computer message system to bully, harass or insult someone is totally unacceptable.
- ✓ As e-mail can be forwarded or inadvertently sent to the wrong person, the same care should be taken with levels of language and contents as for letters or other communications made as a member of the school.
- ✓ Use of the school network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- ✓ Printer may only be used for school related work and activities. Careless or deliberate wasting of paper will result in the students printing facility being withdrawn.

Parental Consent Form - Use of the Internet

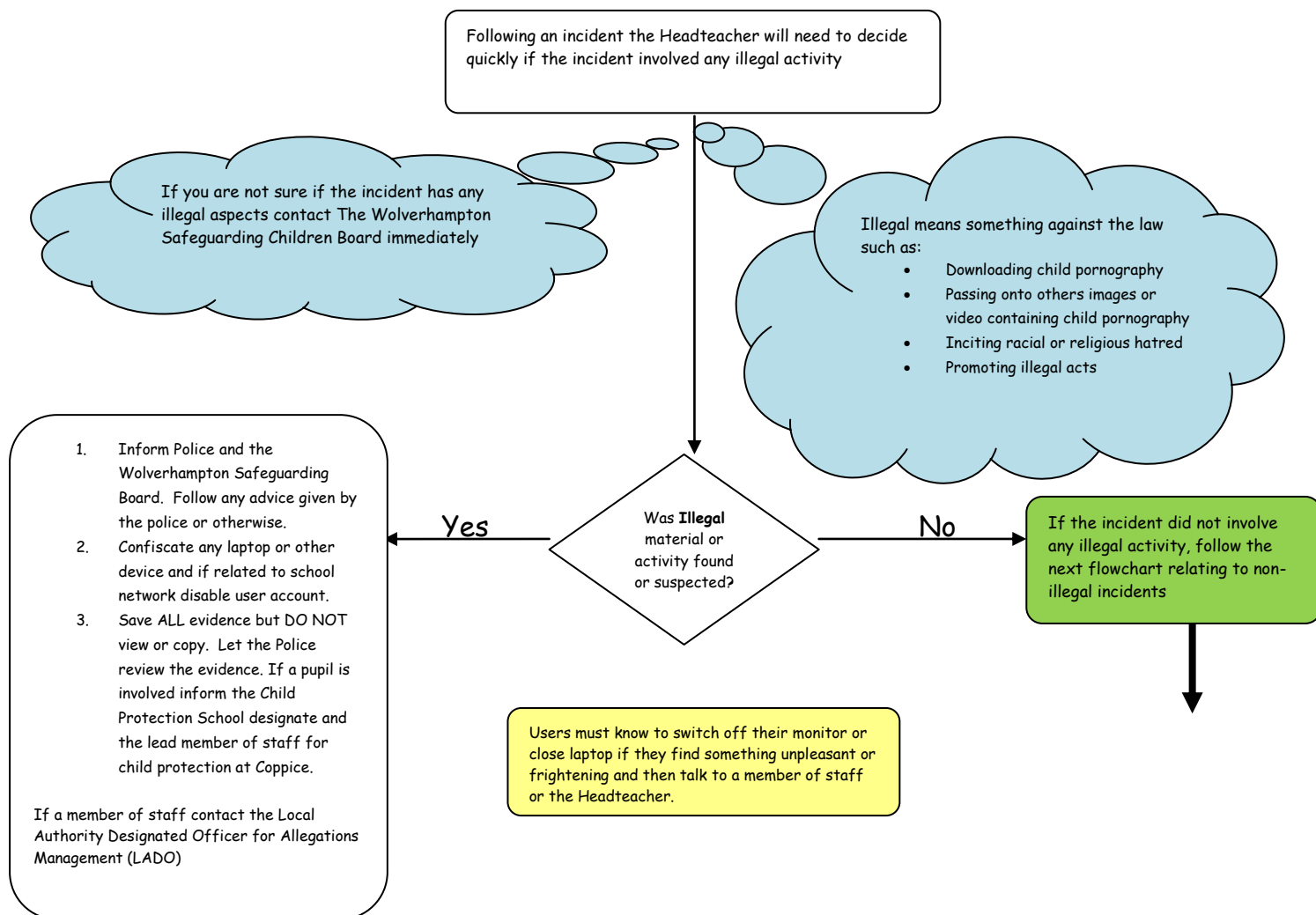
Student Name: _____ Tutor Group: _____

As Parent/Carer of the above student, I give permission for my son/daughter to use computer systems to access the Internet and e-mail. I have read the attached letter and understand that the school will endeavour to take all reasonable steps to restrict access to unsuitable materials on the Internet. I have read the attached Acceptable Use Policy and understand that students will be held accountable for their own actions.

Signature of Parent/Carer: _____

Date: _____

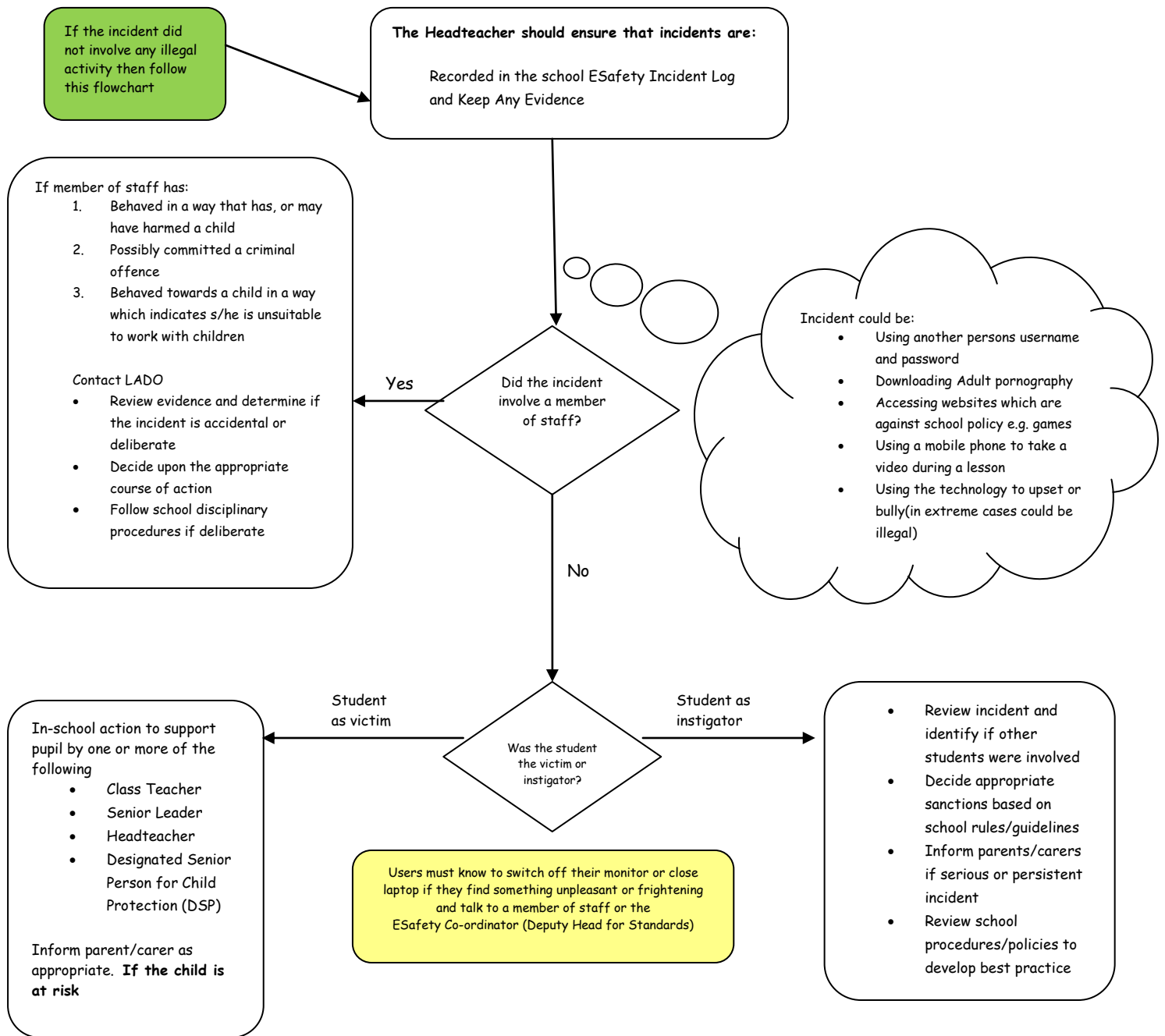
Flowcharts for Managing an ESafety Incident



Key Reminders for Staff working with young people

You Must

- Not communicate with current students on social networking sites
- You must not give personal email addresses or personal mobile phone numbers to students
- You must only use your Coppice School email address to communicate with students and parents
- School devices must not be used to access or store any material that may be deemed inappropriate or illegal



Incident Log

Coppice School ESafety Incident Log

Details of all ESafety incidents to be recorded by ICT support. The incident log will be monitored periodically by the Headteacher or a member of the MLT. Any incidents of Cyber bullying should be recorded and communicated with a member of the LT immediately.

Date & Time	Name of student or staff member	Male or Female	Room and computer / device number	Details of incident (including evidence)	Actions and reasons

Displaying ESafety advice

All parents received advice about e-safety as part of the whole school mailing pack September 2009. This was CD format.

A range of posters are displayed in ICT rooms including CEOP and SMILE.

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

<http://www.hms0.gov.uk/acts/acts1998/19980029.htm>

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

<http://www.hms0.gov.uk/si/si2000/20002699.htm>

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

<http://www.hms0.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998

<http://www.hms0.gov.uk/acts/acts1998/19980042.htm>

Other Acts relating to ESafety

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information

www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining their author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 - 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

ESafety Audit

This self-audit should be completed by the member of the Leadership Team (LT) responsible for ESafety policy. Staff that would contribute to the audit include: Designated Child Protection Coordinator, SENCO, Network Manager and Headteacher.

Has the school an ESafety Policy that complies with Wolverhampton LA and Becta guidance?	Y/N
Date of latest update (at least annual):	
The school ESafety policy was agreed by governors on:	
The policy is available for staff at: www.coppice-school.org.uk	
The policy is available for parents/carers at: www.coppice-school.org.uk	
The responsible member of the Leadership Team is:	JF
The governor responsible for e-safety is:	tbc
The Designated Child Protection Coordinator is:	DF
Has ESafety training been provided for both students and staff?	Y/N
Is there a clear procedure for a response to an incident of concern?	Y/N
Have e-safety materials from CEOP and Becta been obtained?	Y/N
Do all staff sign a Code of Conduct for ICT on appointment?	Y/N
Are all students aware of the School's ESafety Rules?	Y/N
Are ESafety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students?	Y/N
Do parents/carers sign and return an agreement that their child will comply with the School ESafety Rules?	Y/N
Are staff, Students, parents/carers and visitors aware that network and Internet Use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by LT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements?	Y/N
Has the school-level filtering been designated to reflect educational objectives and approved by SLT?	Y/N
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of LT?	Y/N
Have appropriate teaching and/or technical members of staff attended training on the DGFL filtering system?	Y/N