Sydenham School
e-safety
Policy

Updated June 2015

To be reviewed June 2017

AIM HIGH

Achieve Higher

Digital Citizenship & E-Safety Policy

PRINCIPLES

The Internet, digital communication and digital technology are essential elements in 21st century life for education, business and social interaction. As an inner-city Secondary School, we have a duty to provide developmentally-appropriate experiences in ICT in its various forms, to build a foundation on which children can develop their knowledge, skills, understanding and values.

The Green Paper, Every Child Matters, and the provisions of the Children Act 2004, Working together to Safeguard Children, set out how organisations and individuals should work together to safeguard and promote the welfare of children.

The „staying safe‟ outcomes state that children and young people should be:

- Safe from maltreatment, neglect, violence and sexual exploitation
- Safe from accidental injury and death
- Safe from bullying and discrimination
- Safe from crime and anti-social behaviour in and out of school
- Secure, stable and cared for.

Many of these aims apply equally to the virtual world that children and young people encounter whenever they use ICT in its various forms.

This policy outlines the school‟s commitment to e-safety and digital citizenship education as a core part of the school curriculum, clarifies school procedures for monitoring the appropriate use of technology and reducing risk, and states clear procedures for responding to e-safety incidents that may arise.

PURPOSE

- ❑ To develop a culture of digital citizenship and empowerment through technology;
- ❑ To ensure students understand their responsibilities as digital citizens (both in and out of school), so that they are able to manage their online reputation and use ICTs in responsible ways;
- ❑ To ensure parents understand their responsibilities in modelling and promoting digital citizenship in the home, and how they can help to keep their children safe from harm;
- ❑ To advise staff on their responsibilities to develop and model digital citizenship knowledge, understanding, skills and values through the wider curriculum, and to manage and respond to e-safety risks;
- ❑ To ensure all stakeholders understand the school‟s approach to monitoring the appropriate (and inappropriate) use of ICTs and outline sanctions for misuse;

DEFINITION

The school‟s ICT system referred to in this policy encompasses all hardware, software, devices, communications and data that is owned by Sydenham School or connected to the Sydenham School network. This includes all data files that are stored in student and staff work areas which are by definition owned by the school.

The Digital Citizenship and E-Safety policy covers all use of these mediums both inside and outside school (via remote access), but also covers the use of specific knowledge gained as a result of being a member of the school community to publish to websites or other communications media outside school, e.g. on Social Networking Profiles or other digital collaborations. The Policy also covers the use of facilities provided by external organisations when undertaking school trips or visits, and all personal or other technologies used on the school site.

THE BENEFITS OF INTERNET ACCESS FOR EDUCATION

For young people the Internet, and the increasing number of digital devices they use to connect to it, is an integral part of their everyday lives. Whether they use it to express themselves or to stay in touch with friends, for entertainment or education, the Internet can provide tremendous benefits and most use it safely. But while digital technology provides a wealth of opportunities, we are all aware that there are online risks and sometimes these risks can lead to harm. At the same time, while young people‟s „offline‟ and „online‟ worlds are often merging, the behaviours and safeguards of the „real‟ world are not always applied in a „virtual‟ world where friends can be added at the click of button and information shared in an instant.

The risks that children might be exposed to online are:

- Content: harm that can arise from exposure to age inappropriate, distasteful or illegal content;
- Conduct: harm that can arise from how young people behave online;
- Contact: harm that can arise from interactions with other individuals online;

ROLES AND RESPONSIBILITIES

The Role of Governors

- Ensure the role of **e-safety officer** is undertaken by the Designated Child Protection Officer; this is not a technical role;
- Ensure the **safeguarding governor** has an overview of all matters of digital citizenship and e-safety policy;
- Will ensure appropriate training is completed;
- Will ensure ICT usage is monitored appropriately within School and that agreed protocols are being followed in order to respond to e-safety incidents;
- Ensure this policy is reviewed annually by key staff and students;

The Role of Students

Students at Sydenham School are expected to:

1. Contribute to the development and review of the Digital Citizenship and E-Safety Policy and related policies through student voice;
2. Read, understand and agree to the Acceptable Use Agreement and related policies and accepting the agreement at each logon;
3. Adhere to the Digital Citizenship and E-Safety Policy and related policies;
4. Commit to growing and developing their ICT practice, through active involvement in the computing and digital citizenship curriculum;
5. Take responsibility for keeping themselves – and others – safe online;
6. Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies;
7. Assess the personal risks of using any particular technology, and behave safely and responsibly to limit those risks;
8. Respect the feelings, rights, values and intellectual property of others;
9. Seek help from a trusted adult if things go wrong, and support others who may be experiencing e-safety issues;

The Role of Staff

All staff delivering learning or care at Sydenham School have an essential role in creating an e-safe culture. The key responsibilities for all staff are:

1. Contribute to the development of the Digital Citizenship and E-Safety Policy and related policies;
2. Read and adhere to the Acceptable Use Agreement and related policies, and accepting the agreement at each logon
3. Have an awareness of e-safety issues and how they relate to the children in their care;
4. Model good practice in using new and emerging technologies, emphasising positive learning opportunities;
5. Embed e-safety and digital citizenship education in curriculum delivery wherever possible;
6. Remind students of school rules and procedures as required;
7. Monitor student use of the internet and other ICTs within the classroom, and take appropriate action as required;
8. Know when and how to escalate e-safety issues;
9. Maintain a professional level of conduct in their personal use of technology both within and outside school;
10. Take personal responsibility for their own professional development in this area;

The Role of the Senior Leadership team

The Senior Leadership team has statutory responsibilities for child protection and safeguarding, of which e-safety is an aspect. The key responsibilities of the Senior Leadership team are:

1. Develop, own and promote the e-safety and digital citizenship vision to all stakeholders;
2. Develop and publicise the strategy for the implementation and sustainability of e-safety and digital citizenship, making appropriate resources available to support the development of an e-safe culture;
3. Support the Deputy Headteacher in charge of Safeguarding and Inclusion in the development of an e-safe culture;
4. Receive and regularly review e-safety incident logs;
5. Support the Deputy Headteacher in charge of Safeguarding and Inclusion in the appropriate escalation of e-safety incidents;
6. Take ultimate responsibility for e-safety incidents;
7. Report serious e-safety incidents to the governing body;

The Role of the Deputy Headteacher i/c Safeguarding and Inclusion

The key responsibilities of this role are:

- Develop an e-safe culture under the direction of the Headteacher and act as the named point of contact on all e-safety issues;
- Lead on the development of digital citizenship and e-safety with input from all stakeholder groups;
- Promote the e-safety vision to all stakeholders and support them in their understanding of the issues;
- Ensure that e-safety is embedded within continuing professional development for staff and co-ordinate training as appropriate;
- Ensure that e-safety is embedded across the curriculum as appropriate;
- Ensure that e-safety is promoted to parents and carers, and other users of networked resources;
- Maintain an e-safety incident log;
- Monitor and report on e-safety issues to the Senior Leadership team and other agencies as appropriate;
- Develop an understanding of the relevant legislation;
- Liaise with the local authority or other bodies as appropriate;
- Review and update e-safety policies and procedures on a regular basis;

The Role of the Network Manager and ICT Support Team

The key responsibilities for this team are:

- Support the Deputy Headteacher i/c Safeguarding and Inclusion in the development and implementation of appropriate e-safety policies and procedures;
- Provide a technical infrastructure to support e-safe practices, while ensuring that learning opportunities are still maximised;
- Take responsibility for the security of systems and data;

- Report any technical breaches to the Deputy Headteacher i/c Safeguarding and Inclusion and take appropriate action as advised;
- Develop an understanding of the relevant legislation as it relates to the technical infrastructure;
- Liaise with the local authority and other bodies as appropriate on technical infrastructure issues;
- Read and adhere to the Acceptable Use of ICT and E-Safety Policy and related policies;
- Maintain a professional level of conduct in their personal use of technology both within and outside school;
- Take personal responsibility for their own professional development in this area;

The Role of Parents and Carers

The key responsibilities of parents and carers are:

- Contribute to the development of the Acceptable Use of ICT and E-Safety Policy and related policies through the Parent Forum;
- Read the Acceptable Use of ICT and E-Safety Policy and related policies, encourage their children to adhere to them, and adhere to them themselves when appropriate;
- Use technologies provided by the school for parental access safely and appropriately;
- Discuss e-safety issues with their children and support the school in its e-safety approaches by re-enforcing appropriate behaviours at home;
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies;
- Model appropriate use of new and emerging technologies;
- Liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online;

E-SAFETY & DIGITAL CITIZENSHIP EDUCATION

All users must be active participants in e-safety and digital citizenship education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies.

Sydenham School recognizes the importance of educating our young people on how to stay safe online, and is committed to providing a stimulating curriculum to deliver e-safety and digital citizenship through Computing, PSHE and Citizenship lessons, as well as across the curriculum. All school staff should model safe and appropriate practices across the curriculum whenever technologies are used.

All teaching staff at Sydenham School receive annual safeguarding training which includes e-safety, and are committed to supporting every student in providing opportunities to use ICTs in a safe and responsible manner. We are also committed to providing regular opportunities to help staff consider their own safe use of ICT and the implications of its use.

We also recognize the importance of providing advice and guidance to parents and carers and how to encourage safe use of the Internet and other technologies in the home, and regularly publish such materials through the school website, newsletter and at various events, including parents evenings.

WHOLE-SCHOOL NETWORK SECURITY STRATEGIES

The school‟s computer network security systems are reviewed regularly by the Network Manager.

Network use is routinely monitored by the Network Manager and team. Regular reports are provided to the Senior Leadership team, which may result in appropriate disciplinary action being taken.

Uploading and downloading of non-approved application software is denied.

All access to the school network requires entry of a recognised User ID and password. Staff and students must log out after every network session. All users are responsible for ensuring they use strong passwords and to change their password regularly at least every three months, and are given advice and guidance on this annually by the Network manager.

Virus protection software is installed and updated weekly by the Network Manager.

Using personal USB pen drives is at the user‟s risk, and it is expected that all staff and students will have adequate virus protection on home computers if they choose to use this method of transferring files.

Unapproved system utilities software and executable files are not allowed to be stored in storage areas.

Random checks are made on files held on the school‟s network by the Network Manager. Additional checks will occur if a cause for concern is raised.

Hardware and software infrastructures

The school has invested in the following hardware and software infrastructures to reduce risks associated with the Internet.

- LightSpeed Filtering List – list of school-restricted websites (broken down by category) which can not be accessed at any time, and logs which websites are visited or searched for.
- Impero software – which enables classroom teachers to monitor usage and take action in class, as well as tools to support teaching & learning;

Classroom management structures

Staff are encouraged to make use of the following for managing and monitoring ICT use at the classroom-level:

- Seating plans allow teachers to trace and monitor student access and usage of the Internet;
- Where possible, teachers ensure that computers/ devices are positioned in such a way that screens are easily observed by teachers;
- Classroom monitoring software (Impero) will be used by teachers to further monitor activity and restrict access to websites and/ or software that are not specifically required in a particular lesson;
- Teachers issue sanctions for misuse of ICT systems as per the school Behaviour Policy, and escalate serious incidents as required;
- Staff report any failings of the school ICT infrastructure to the Network Manager and ICT support team as soon as they arise;

RISK ASSESSMENT AND MANAGEMENT OF INTERNET CONTENT

The school takes all reasonable precautions to ensure that students access appropriate material only. However, it is not possible to guarantee that a student will never come across unsuitable material while using a school networked device. The school cannot accept liability if such material is accessed nor for any consequences resulting from Internet access.

All students are taught effective online research techniques, including the use of search engines. Receiving information over the web or in e-mail or text messages presupposes good information-handling skills.

Key online information-handling skills include:

- Ensuring the validity, currency and origins of the information accessed or received;
- Using alternative sources of information for comparison purposes;
- Identifying an author‟s name, date of revision of the materials, and possible other links to the site;
- Respecting copyright and intellectual property rights.

Students will be made fully aware of the risks to which they may be exposed while on the Internet. They will be shown how avoid the negative areas of the Internet such as pornography, violence, racism and exploitation of children, and follow a comprehensive Digital Citizenship and e-Safety education programme which is embedded within the Computing and PSHE curriculum, as well as cross-curricular links.

However, if they encounter such material they will know that they should switch off the monitor (where possible), not the computer, and report the incident to the nearest teacher or the school's Network Manager who will deal with it according to the school AUP.

REGULATION AND GUIDELINES

The school‟s Internet access incorporates a filtering system (LightSpeed) to block inappropriate websites. The filtering system used on the school network aims to achieve the following:

- Access to inappropriate or illegal sites is blocked at all times;
- Additional web or software filtering may be undertaken by the classroom teacher (Impero);
- Records of Internet sites visited by students and teachers are logged;

The Network Manager regularly assesses the effectiveness of the filtering system.

The Network Manager will immediately report the details of any inappropriate or illegal Internet material found to have been accessed by students to the Deputy Headteacher for Safeguarding and Inclusion.

The Network Manager will immediately report the details of any inappropriate or illegal Internet material found to have been accessed by staff to the Headteacher.

ICT Rules

A list of rules is displayed in all classrooms and workspaces that have a networked computer. This states that user‟s must not:

- Interfere with any other student’s device
- Send inappropriate e-mails or messages that may cause offence or discomfort to others
- Photograph or film any person without their knowledge and consent
- Publish inappropriate content to the web
- Access obscene or indecent material
- Infringe the copyright of another
- Deliberately access unauthorised network drives or blocked content (hacking)
- Damage or interfere with equipment
- Use technology for any other inappropriate purpose as determined by the school

Sydenham’s e-presence (via our website, e-newsletters, twitter feed or blogs)

Pupils' work published through Sydenham‟s e-presence will not be identified by their surnames.

Including photographs of groups of pupils on the school website can be motivating for the pupils involved, and provide a good opportunity to promote the work of the school. Such photographs will only be used for educational purposes and the identity of children will be protected. The full name of a pupil will never be included alongside the photograph.

Parental permission is sought at the time of entry to the school for the use and publication of pupils‟ photographs.

Personal information concerning pupils will not be disclosed or used in any way on the school website without the specific permission of a parent or guardian. Pupils are not permitted to provide private or confidential information about themselves or others on the Internet.

More information on safeguarding students can be found in the Safeguarding Policy.

Moderated mailing lists and Web 2.0 technologies

The school uses an e-mail distribution list to send messages to selected groups of users.

Teachers will moderate other collaboration tools (known as Web 2.0) such as the discussion forums, wikis and blogs located on the school‟s Virtual Learning Environment (Frog). These are to be used on the school network for learning purposes only.

Bring Your Own Device (BYOD) programme & Other communication technologies

The school plans to implement a BYOD programme in the coming years, which will enable students to utilise personal tablet devices or laptops in the classroom for the purpose of learning.

In order for students to partake in this scheme, the device must meet the school‟s minimum requirements for these devices and agree to install the Impero client software on to the device. They will then be asked to connect to an Impero session in lesson time in order to provide the teacher with the ability to monitor usage and to use a range of teaching & learning tools with them. Students who refuse to install the Impero client or to join an Impero session will not be permitted to utilise their device in lessons.

Students are not allowed to use other personal devices (such as mobile phones, handheld games consoles and MP3 players) during lessons. These devices should be kept out of site and in silent mode during these times, and the school will confiscate such items if found.

The school will also seek to confiscate such items where they suspect they have been used in illegal activity or other e-safety incidents. These will be secured and evidence preserved for the appropriate authorities.

Where the school provides students with additional devices for the purpose of learning (e.g. Digital Cameras, Digital Video Cameras, Webcams, Digital Dictaphones etc), these should be used only for the purpose provided and their use will be monitored by teaching staff.

It is forbidden to use the school network to send abusive or otherwise inappropriate text messages or other communications using the facilities provided by the school network.

The use of mobile and other personal devices by staff in school is entirely at the user‟s risk.

Students with Special Educational Needs or Particular Vulnerability

The Staying Safe Action Plan 2008 identified that targeted safeguarding is needed for some groups of children who are at greater risk than others. The school will therefore pay particular attention to the online activities of these students through additional monitoring.

COMMUNICATING THE SCHOOL’S AUP

Informing students

AUP posters are displayed near all networked computer systems. Students are informed that their Internet use is monitored and given instructions on safe and responsible use of the Internet through Assemblies and lessons. The Student agreement form that students and their parents must sign each year is contained within the student planner. Students must also accept this agreement on screen before being allowed network access.

Informing staff

All staff are provided with electronic access to this policy. Teachers are aware that Internet traffic can be monitored and traced to an individual user. All staff complete a CRB check prior to gaining access to the school‟s Management Information System, VLE and Shared Resources.

All users agree to comply with this policy by logging on to the school computer system, and this is clearly displayed on the logon screen.

Informing parents / carers

Parents‟ attention has been drawn to the School AUP through the school newsletter, VLE and on the school‟s website. Advice that accords with acceptable and responsible Internet use by students at home will be made available to parents. Safety issues will be handled sensitively.

All comments on and suggestions concerning this Acceptable Use Policy should be sent to the Deputy Headteacher for Safeguarding and Inclusion.

CONSEQUENCES OF VIOLATING THE SCHOOL’S AUP

Student Violations

Most violations of the school‟s AUP by students will be dealt with via the school behaviour policy. Teaching staff will issue demerits and the associated sanctions for failing to comply with the ICT rules displayed in each classroom.

However, in some situations, the breach will be more serious and require additional sanctions to be applied. Staff will report the following more serious incidents to the Deputy Headteacher i/c Safeguarding and Inclusion:

- Accidental or deliberate access to inappropriate/ obscene material, e.g. pornography
- Accidental or deliberate access to illegal material, e.g. child pornography
- Serious cyber-bullying or harassment using technologies
- Sexual exploitation using technologies, e.g. sexting

Racist or Homophobic Abuse will be dealt with via the school‟s Equality and Diversities Policy as usual.

If a student is found to have intentionally violated the school‟s AUP following an investigation by the school, the school‟s behaviour policy is followed and actions in the amber and red sections may be carried out (this can include permanent exclusion should the need arise)

Removal of network or other privileges (e.g. Internet Access, Email Access) will rarely be used as a sanction as this will inevitably hamper student progression in the Computing curriculum, as well as in other curriculum areas.

The Deputy Headteacher in charge of Safeguarding and Inclusion will keep an e-safety incident log and will report serious breaches of the AUP to the appropriate authorities. This may involve one or more of the following actions:

- Reporting illegal activity to local police
- Reporting sexual abuse and exploitation to the Child Exploitation and Online Protection Centre (CEOP)
- Reporting illegal online content to the Internet Watch Foundation (IWF)
- Reporting child protection issues to the LSBC and Social Services

Staff Violations

All violations of the school‟s AUP by staff will be reported to and investigated by the Headteacher. These will then be dealt with via the Staff Discipline Policy or Staff Capability Policy as appropriate.

Serious breaches of the school AUP may also require the evidence of this breach to be referred on to the local Police or other appropriate bodies (as detailed for students above).

Parent Violations

Parents who violate the school‟s AUP whilst using the VLE, will have their access to this service revoked, and may also require the evidence of this breach to referred on to other appropriate bodies (as detailed for students above).

REVIEWING THIS POLICY

As a result of the rapid development of new technologies and the frequently changing nature of their use within society, the school is committed to regularly reviewing and updating this policy in response to e-safety incidents, new legislation and Local Authority advice.

The policy has been developed in light of the February 2009 advice document from Becta, the June 2008 report from the UK Council on Child Internet Safety (UKCCIS), the March 2008 Byron Review on "Safer Children in a Digital World", and the January 2014 Ofsted "Inspecting e-Safety in Schools" briefing.

REFERENCES TO OTHER POLICIES

This policy links directly to the school‟s Anti-Bullying Policy, Freedom of Information Policy, Behaviour Policy and Equalities & Diversities Policy.

LIST OF APPENDICES

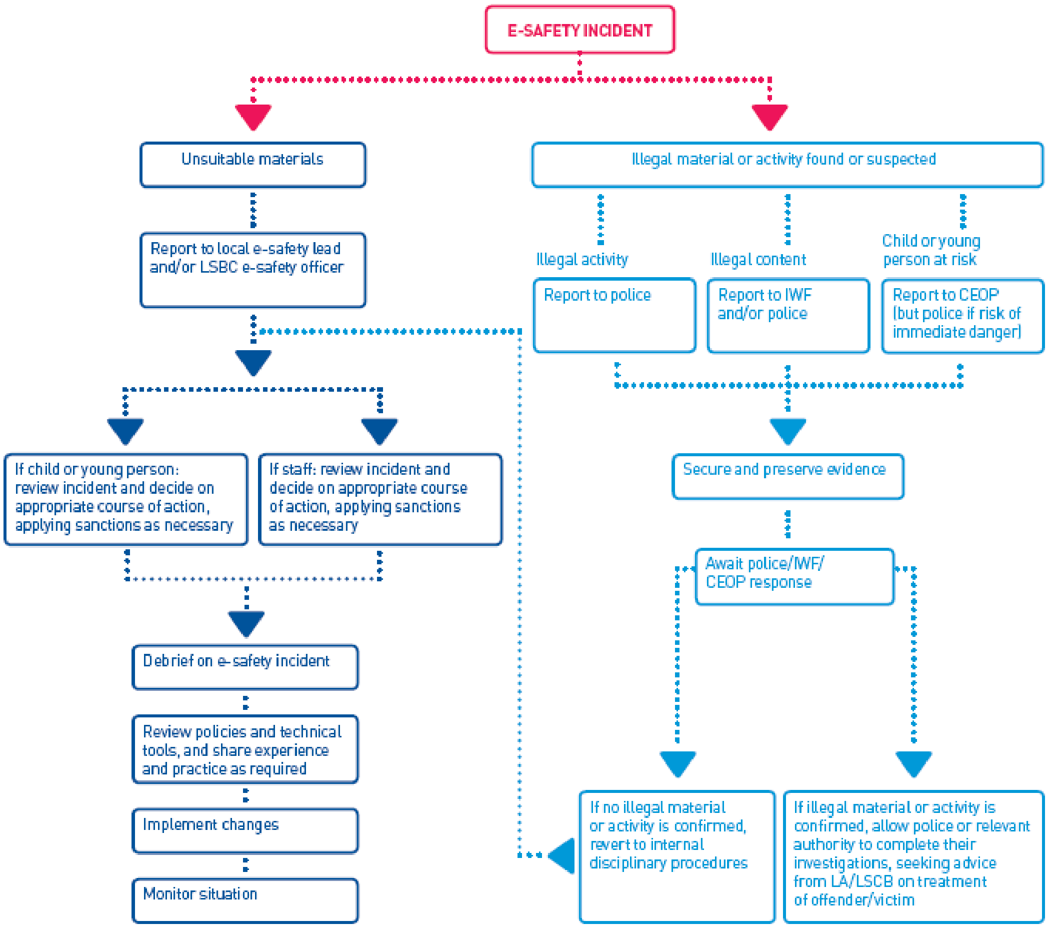
APPENDIX ONE – E-SAFETY INCIDENT REPORTING FLOWCHART

This flowchart indicates the courses of action that should be taken by the Deputy Headteacher i/c Safeguarding and Inclusion on receipt of a reported e-safety incident.

Unsuitable materials – refers to students accessing non-illegal, but inappropriate materials.

Illegal material or activity – refers to any incident where a staff member or student may have accessed, created or transmitted illegal materials, or been actively involved in an activity which may be considered illegal. (see appendix four).

Flowchart for responding to e-safety incidents



E-SAFETY INCIDENT
Unsuitable materials
Report to local e-safety lead and/or LSBC e-safety officer
If child or young person: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Debrief on e-safety incident
Review policies and technical tools, and share experience and practice as required
Implement changes
Monitor situation
Illegal material or activity found or suspected
Illegal activity
Illegal content
Child or young person at risk
Report to police
Report to IWF and/or police
Report to CEOP (but police if risk of immediate danger)
Secure and preserve evidence
Await police/IWF/ CEOP response
If no illegal material or activity is confirmed, revert to internal disciplinary procedures
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LA/LSCB on treatment of offender/victim

APPENDIX TWO – STUDENT AGREEMENT

Sydenham School — Student ICT Agreement

The Internet, digital communication and digital technology are essential elements in 21st century life for education, business and social interaction. Unfortunately though, there are times when internet and computer misuse can have a negative effect on students' learning.

In order for all students' to benefit fully from the wide availability of ICT resources, we expect you to use facilities in a responsible manner at all times and ask you to read and sign the following statement.

Students must not:

- **Interfere with any other student's device**
- **Send inappropriate e-mails or messages that may cause offence or discomfort to others**
- **Photograph or film any person without their knowledge and consent**
- **Publish inappropriate content to the web**
- **Access obscene or indecent material**
- **Infringe the copyright of another**
- **Deliberately access unauthorised network drives or blocked content (hacking)**
- **Damage or interfere with equipment**
- **Use technology for any other inappropriate purpose as determined by the school**

The school's ICT-based resources and all information contained therein (including material found in student areas) is and will remain the property of Sydenham School.

All Internet use is logged and the school regularly exercises its right to monitor the use of the school's computer systems. This includes the interception and monitoring of e-mail. Files will be subject to deletion if unauthorised use of the school's computer system is or may be taking place. Users should not expect that files stored on servers or disks to be in any way private and be mindful of this when using these resources.

It is your responsibility to prevent inappropriate access to your files by not publicising or giving anyone else your passwords, and to keep regular backups of your work. The school can not be held accountable for any files that are accidentally deleted or lost as the result of negligence on the student's behalf.

If you accidentally access material that is prohibited by this agreement, you should immediately turn off your screen (not the computer), and report this to the supervising staff member as soon as possible. Failure to do this will result in the breach being deemed intentional.

If you are the victim of cyberbullying or digital harassment, or have any concerns of this kind, you should report this to your tutor who will be able to give advice or seek further support for you.

The following statements reflect the school's Digital Citizenship and E-Safety Policy and outline the standards and attitudes we expect from students when using Sydenham School's ICT systems.

Sydenham School — Digital Citizenship and e-Safety Education

Sydenham School recognizes the importance of educating our young people on how to stay safe online, and is committed to providing a stimulating curriculum to deliver Digital Citizenship and e-Safety through Computer Science, PSHE and Citizenship lessons, as well as across the curriculum. All school staff model safe and appropriate practices across the curriculum whenever technologies are used.

All teaching staff at Sydenham School receive annual safeguarding training which includes modules on e-safety, and are committed to supporting every student in providing opportunities to use technology in a safe and responsible manner.

We also recognize the importance of providing advice and guidance to parents and carers on how to encourage safe use of the Internet and mobile technologies in the home, and regularly publish such materials through the school website, newsletter and learning gateway, and at parents' evenings. We run an annual e-Safety session as part of the Parent Forum, which is supported by Childnet International.

For further guidance and support, we recommend parents visit the Childnet International website at: http://www.childnet-int.org/kia/

Sydenham School — Internet Usage Parental Permission Form

Please complete and return this form to Reception.

Student Statement

Student name: ………………………………………………………………………… Tutor Group: ………………………

I have read and understand the above rules and agreed to comply with them. I understand that failure to comply may lead to the removal of my access rights and any further sanction that the management of the school imposes, including exclusion or permanent exclusion from the school for a serious offence or repeated minor offences.

Student signature: ……………………………………………………………………… Date: ……………………………………………

Parent Statement

Parent / Guardian name:
………

As a parent or legal guardian of the above pupil, I grant permission for my daughter to use electronic mail and the Internet. I have read, understood and agree to what my daughter has signed. I understand that students will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my daughter to follow when selecting, sharing and exploring information and media.

Parent / Guardian signature: ………………………………………………………… Date: ……………………………….

APPENDIX THREE – DEALING WITH AN INCIDENT (ADVICE FOR STAFF)

Where any of the following prohibited actions are observed by a member of staff:

Observed pupil action	**Staff action (in all cases log on e-portal)**
Using a mobile phone during lessons/in a classroom	Confiscate the phone and pass to Head teacher‟s PA
Using Facebook, twitter or other instant messaging systems	It is illegal for under-13s to use Facebook – this must be reported to parents via Curriculum Leader/Year Learning Coordinator For other actions where pupils have been told not to use them during a lesson normal school behaviour procedures apply
Students trying to access pornography or other inappropriate images	Students should be moved away from the screen and the screen switched off (rather than PC turned off) Member of ICT Support should be called to record images and ascertain how they were accessed and these can also be used as part of reporting to parents. Senior member of pastoral staff (YLC or „above‟) should manage the incident Designated Child Protection Officer (Jacqui O‟Connor) should be informed.
Cyberbullying	Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying. • There will be clear procedures in place to support anyone affected by Cyberbullying. • All incidents of cyberbullying reported to the school will be recorded. • There will be clear procedures in place to investigate incidents or allegations of Cyberbullying: • Students, staff and parents/carers will be advised to keep a record of the bullying as evidence. • The school will take steps to identify the bully, where 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 as set out in the school's behaviour policy • The Police will be contacted if a criminal offence is suspected.

See the Behaviour Policy and consult members of the Senior Leadership Team for further advice.

Logging of incidents

e-portal

All behavioural incidents should be recorded on e-portal in the usual manner and sanctions put in place in consultation with relevant personnel (usually Subject or Curriculum Leader).

Where appropriate the (new category) „use of electronic messaging‟ should be used alongside other relevant categories

Other agencies

If you are very concerned then the Designated Child Protection Office (Jacqui O‟Connor) or her deputies (Linda Lambird and Sid Robinson) will advise you if a matter needs to be reported to the police or other external agencies and will do the reporting.

APPENDIX FOUR – APPLICABLE LEGISLATION

Acts relating to monitoring of staff email

Data Protection Act 1998 – www.hsmso.gov.uk/acts/acts1998/19980029.htm
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.

Telecommunications (Lawful Business Practice and Interception of Communications) Regulations 2000 – www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000 – www.hmso.gov.uk/acts/acts2000/20000023.htm
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.

Human Rights Act 1998 – www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to e-Safety

Racial and Religious Hatred Act 2006 – www.opsi.gov.uk/acts/acts2006/ukpga_20060001_en_1
It 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 – www.opsi.gov.uk/acts/acts2003/ukpga_20030042_en_1
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.

Communications Act 2003 (Section 127) –
www.opsi.gov.uk/acts/acts2003/ukpga_20030021_en_1
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.

Computer Misuse Act 1990 – www.opsi.gov.uk/acts/acts1990/ukpga_19900018_en_1.htm
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 persons 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 –
www.opsi.gov.uk/acts/acts1988/ukpga_19880027_en_1.htm
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 –
www.opsi.gov.uk/acts/acts1988/ukpga_19880048_en_1.htm
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 them 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) – www.opsi.gov.uk/si/si1987/uksi_19870198_en_2.htm
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) –
www.opsi.gov.uk/revisedstatutes/acts/ukpga/1978/cukpga_19780037_en_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 –
www.opsi.gov.uk/revisedstatutes/acts/ukpga/1964/cukpga_19640074_en_1
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997 – www.opsi.gov.uk/acts/acts1997/ukpga_19970040_en_1

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.

APPENDIX FIVE

Sydenham School
Internet Policy for Staff

This policy is an appendix to Sydenham School‟s Digital Citizenship and E-Safety Policy (AUP).

The aim of Sydenham School‟s Acceptable Use of ICT and E-Safety Policy (AUP) is to acknowledge and clarify the school's role in providing safe and appropriate technologies and e-safety education and ensure it is appropriate to the school and pupils' needs. The policy provides information about procedures in response to any e-safety incident and provides guidance to teachers, support staff and outside visitors.

Our Acceptable Use Policy ensures that our school takes a whole-school approach on the issue of e-safety as part of the commitment to being a healthy school. Staff need to be confident and skilled to teach e-safety, and pupils who are concerned about their safety online need to be supported.

General Principles

The Internet is an excellent tool for research and can be great fun. However there may be a temptation to use it too much or to access inappropriate sites. Sydenham School‟s policy is designed to enable proper use of the Internet and to clarify what is unacceptable.

1) Sensible use of the Internet

The use of the Internet **during work time** should be **for work-related purposes only**. You may use the Internet for private use during your own time, e.g. during breaks, lunch and outside of the agreed contracted hours of work.

It is unacceptable to use or encourage anybody else to use the Internet or your user account to access or surf:

- pornographic sites
- sites encouraging racist behaviour
- sites encouraging homophobic behaviour
- sites which have material of a sexual or sexually provocative nature
- sites of violence
- paedophilia
- other chid abuse
- abuse of animals

2) Use of e-mails from work place

The author of any e-mail from Sydenham School must be readily identified. All staff members must have a signature enclosed in sent emails, clearly detailing their name, role and school contact information.

You should not access private accounts during work time except for work-related use.

You must keep your email account to a reasonable size. IT support staff will delete emails and other files, under instruction from the Senior Leadership Team, and reserve the right to delete emails and other files if the size limit is exceeded.

You must notify the network manager immediately if you receive inappropriate material through surfing the Internet or via your e-mail accounts.

You must ensure that appropriate action is taken to prevent others from accessing your email account or use your user area.

3) Downloads and mailing lists

You may not download any software or utilities without the express permission of the Network Manager.

You may download PDF files or other documents from reputable sources.

You may put yourself on mailing lists but you should remove yourself if you no longer want to subscribe. If you leave Sydenham School, IT support staff can access users email and their areas by changing the users password. This will enable them to remove you from any remaining mailing or distribution lists. In addition, your emails will be deleted and your mailbox closed as soon as the member of staff is off roll.

4) Monitoring use of IT Systems

The Senior Leadership Team has the right to monitor the use of Sydenham School‟s ICT systems to avoid abuse or any inappropriate use of the internet.

As a result of this monitoring, the school will aim to support staff in breach of this policy by offering appropriate safeguarding training to include e-safety issues, providing advice/ guidance around appropriate protocols and also offer opportunities to discuss implications of the internet.

We will seek to balance privacy with the requirements to monitor adherence to this policy. Incidents of inappropriate use will be raised individually with members of staff privately, but will be shared with Human Resources. A record of these will be kept.

5) Disciplinary procedures should staff be found to be using the net in an inappropriate way.

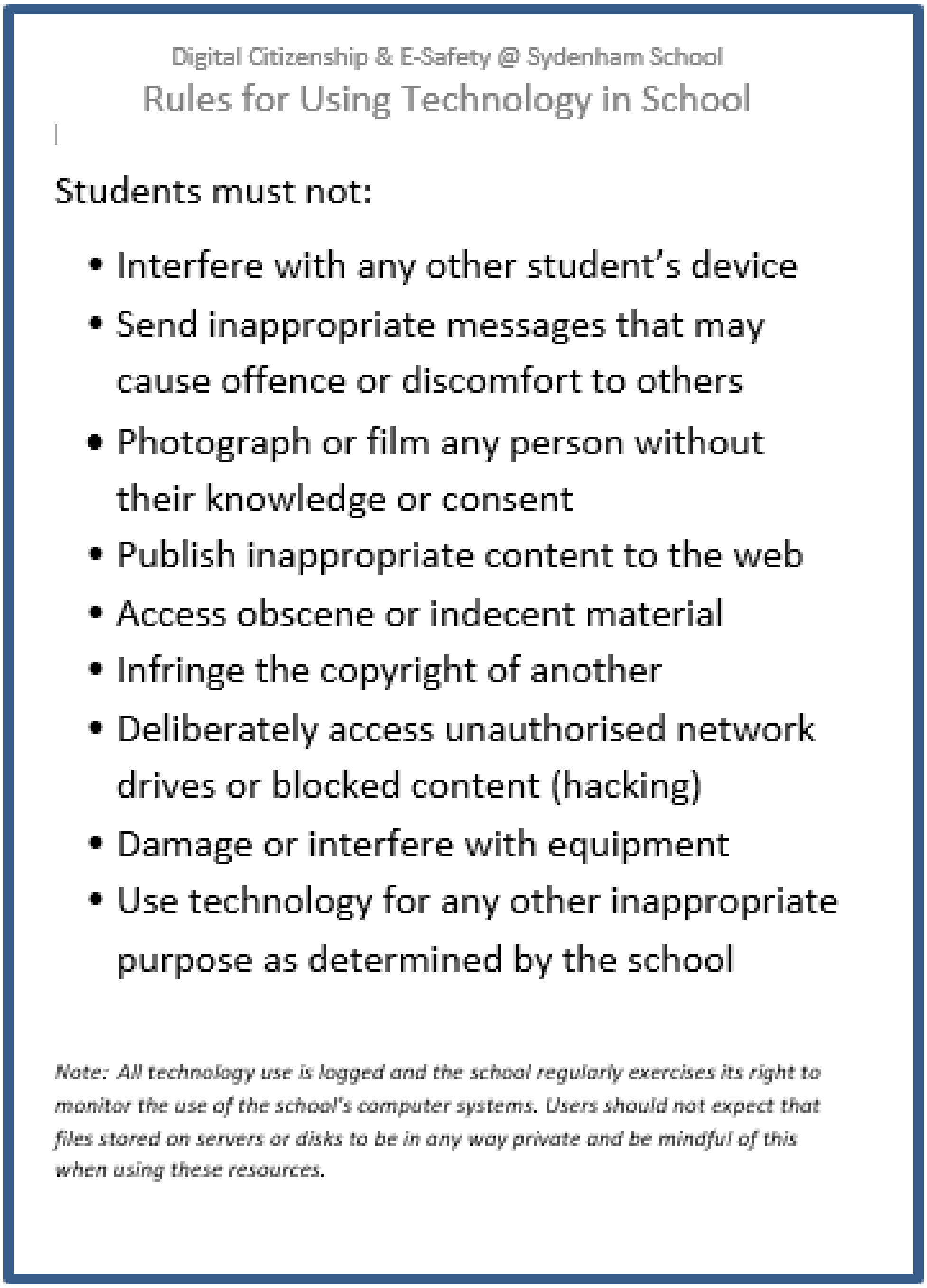
It is a disciplinary offence to use Sydenham School‟s IT systems or the Internet in an inappropriate way or in a way that breaches this policy. The main purpose of the disciplinary procedure is to encourage an employee whose conduct is unsatisfactory to improve. (See Disciplinary Procedure)

It must be stated that staff should be aware and must consider the implication in their use of the internet outside school. This awareness should include their own protection (e.g. not sharing personal details, not communicating with students through unofficial systems, not communicating with pupils through social networking sites, the risks to personal career if inappropriate images/ videos/ details about them are made known and distributed). This needs to be considered so that both staff and pupils are safeguarded.

6) Consequences of breach of policy

The appropriate disciplinary procedures may be activated. Disciplinary action may, at its extreme, lead to dismissal should there be a breach of this agreed policy.

Appendix Six – School ICT Rules Poster



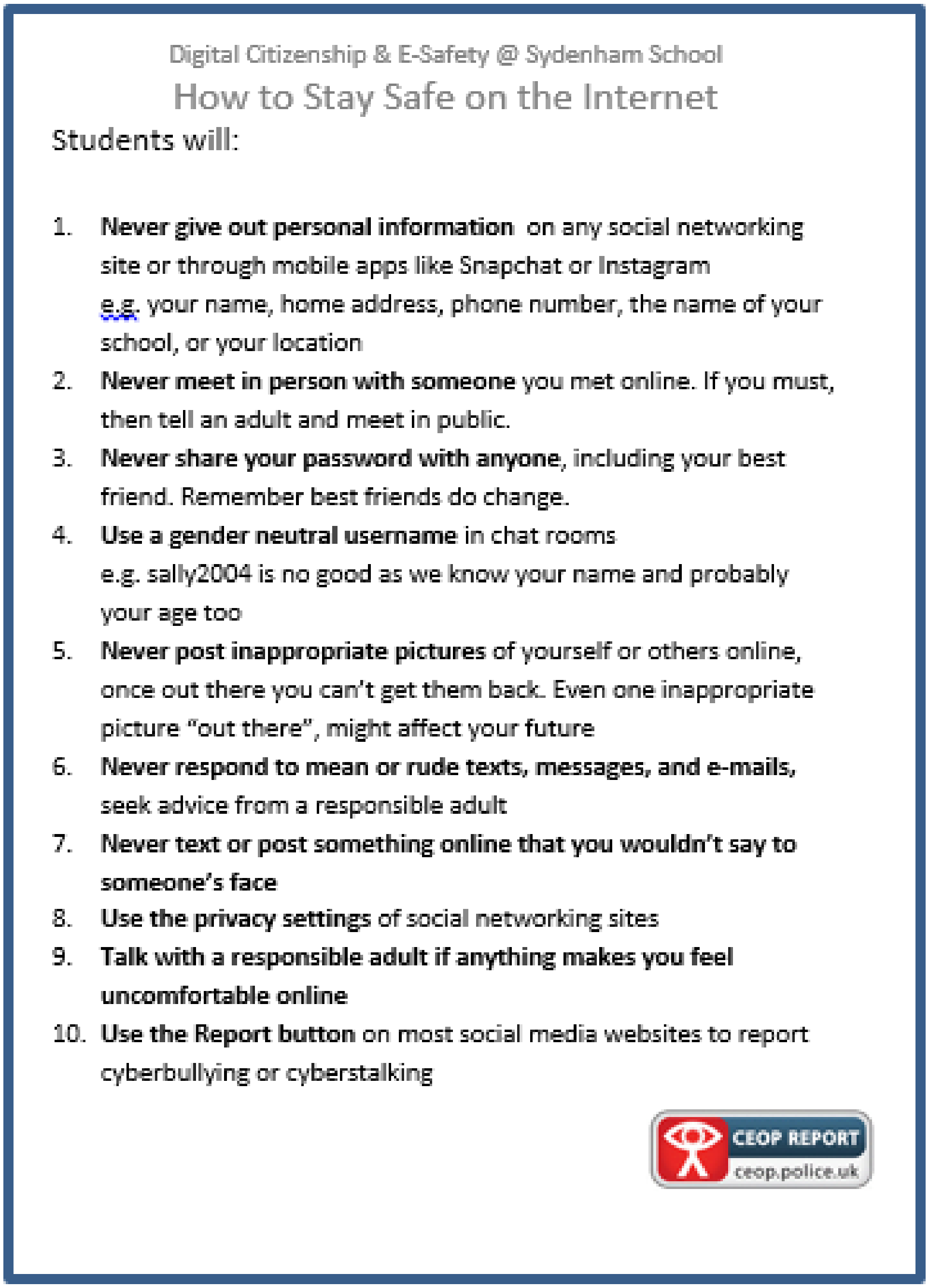
Digital Citizenship & E-Safety @ Sydenham School

Rules for Using Technology in School

Students must not:

- Interfere with any other student's device
- Send inappropriate messages that may cause offence or discomfort to others
- Photograph or film any person without their knowledge or consent
- Publish inappropriate content to the web
- Access obscene or indecent material
- Infringe the copyright of another
- Deliberately access unauthorised network drives or blocked content (hacking)
- Damage or interfere with equipment
- Use technology for any other inappropriate purpose as determined by the school

Note: All technology use is logged and the school regularly exercises its right to monitor the use of the school's computer systems. Users should not expect that files stored on servers or disks to be in any way private and be mindful of this when using these resources.



Digital Citizenship & E-Safety @ Sydenham School

How to Stay Safe on the Internet

Students will:

1. **Never give out personal information** on any social networking site or through mobile apps like Snapchat or Instagram e.g. your name, home address, phone number, the name of your school, or your location
2. **Never meet in person with someone** you met online. If you must, then tell an adult and meet in public.
3. **Never share your password with anyone**, including your best friend. Remember best friends do change.
4. **Use a gender neutral username** in chat rooms e.g. sally2004 is no good as we know your name and probably your age too
5. **Never post inappropriate pictures** of yourself or others online, once out there you can't get them back. Even one inappropriate picture "out there", might affect your future
6. **Never respond to mean or rude texts, messages, and e-mails,** seek advice from a responsible adult
7. **Never text or post something online that you wouldn't say to someone's face**
8. **Use the privacy settings** of social networking sites
9. **Talk with a responsible adult if anything makes you feel uncomfortable online**
10. **Use the Report button** on most social media websites to report cyberbullying or cyberstalking

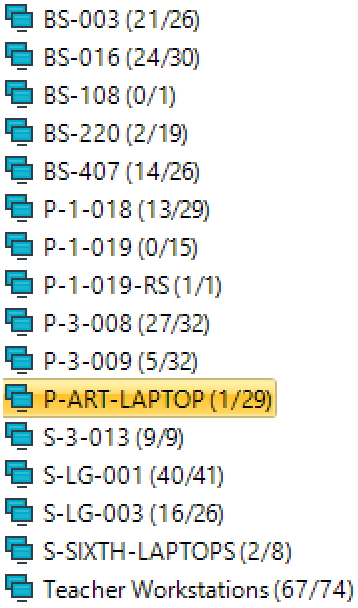
CEOP REPORT
ceop.police.uk

Appendix Seven – Guide to using Impero

Step 1: Open Impero from the Desktop

Impero Console

Step 2: Select a Room or Group of PCs from the left hand menu



- BS-003 (21/26)
- BS-016 (24/30)
- BS-108 (0/1)
- BS-220 (2/19)
- BS-407 (14/26)
- P-1-018 (13/29)
- P-1-019 (0/15)
- P-1-019-RS (1/1)
- P-3-008 (27/32)
- P-3-009 (5/32)
- P-ART-LAPTOP (1/29)
- S-3-013 (9/9)
- S-LG-001 (40/41)
- S-LG-003 (16/26)
- S-SIXTH-LAPTOPS (2/8)
- Teacher Workstations (67/74)

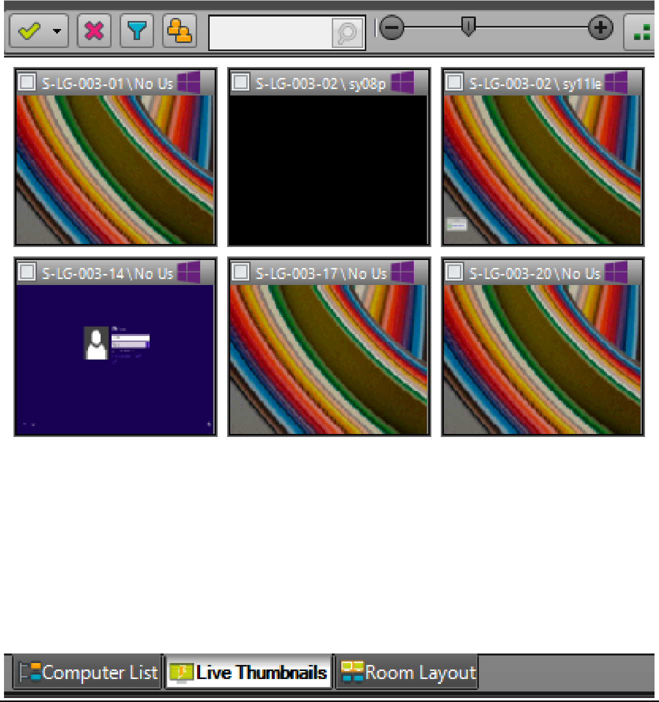
Step 3: Apply group policies from the Group menu that affect all computers in the group, including:

Lock Group	**Lock Group:** Locks the screens so that the devices cannot be used, until the Unlock Group button is clicked.
Lock Internet	**Lock Internet:** Disables access to all websites and other content through a browser, until the Unlock Internet button is clicked.
Disable Printer	**Disable Printer:** Prevents students from printing to any network or local printer, until the Enable Printer button is clicked.
Mute Sound	**Mute Sound:** Disables all sound controls on the device, including through headphones, until the Unmute Sound button is clicked.
Disable USB Storage	**Disable USB Storage:** Prevents users from accessing USB storage devices for loading/ saving/ viewing files, until the Enable USB Storage button is clicked.
Block List	**Block List** Enables you to add to or remove from a list of blocked windows, websites or applications for this group.
Allow List	**Allow List** Enables you to add to or remove from a list of blocked windows, websites or applications for this group.

Step 4: Use the Screen controls to monitor, control or broadcast to selected screens

✓ ▾	Tick each screen manually or use the tick tool to select all machines
Broadcast Screen	**Broadcast Screen** Mirror your PC (or another user‟s device) on all ticked devices until the End Broadcast button is clicked.
Record Screen ▾	**Record Screen** Record part of the whole of your screen (or another user‟s device) for demonstration purposes or collection of evidence.
View/Control ▾	**View/ Control** Open a user‟s screen to see what they are doing or take control of their keyboard/ mouse. This can also be done by double clicking on the thumbnails.

Step 5: Click Live Thumbnails to see what users are doing in the room



Step 6: Use the Action menu to communicate with users or to perform various teaching & learning actions

Send Message	**Send Message** Send an onscreen message to all ticked users.
Live Chat/Forum	**Live Chat/ Forum** Launch a chat facility that all ticked users can contribute to.
Send File	**Send File** Distribute a file, e.g. Word document/ PowerPoint presentation etc, to all ticked devices, and set it to open on their screens.
Collect Files	**Collect Files** Send a request to students for them to submit one or more files to you using a Browse dialog box.
Assign Task	**Assign Task** Provides a list of tasks to be completed for students to tick off. You can view their progress with these tasks on your screen.
Quick Question	**Quick Question** Distribute an electronically completed multiple choice, Yes/ No or Written Answer question for students to complete. You can view responses once submitted.

Finally: Remember to remove any changes you have made before you leave the room, otherwise they will apply for the next teacher.

Appendix Eight – e-Safety Incident Log

E-Safety Incident Log sheet

Please complete this log for all incidents of a bullying, discriminatory or abusive nature involving e-technology, mobile phones, internet etc or more traditional forms i.e. face-to-face, whether students or adults. Incidents where there has been access to inappropriate material on the internet should also be recorded here. **Please note this does not replace referring incidents as appropriate to the local authority, police or children's services as per the e-safety incident flow chart.**

Date	Type of incident	Method used	Action taken	Outcome (with date)

Date	Type of incident	Method used	Action taken	Outcome (with date)

APPENDIX NINE – FURTHER ADVICE & GUIDANCE

Child Exploitation and Online Protection Centre (CEOP) – www.ceop.gov.uk
CEOP is a police organisation focused on the protection of children and young people from sexual abuse and exploitation. It has a broad remit and range of functions to help tackle the sexual abuse and exploitation of children primarily where the use of technology is a factor.

CEOP provides an online facility for the public reporting of any sexually inappropriate or potentially illegal online activity towards a child or young person.

Thinkuknow – www.thinkuknow.co.uk
An education programme being rolled out by CEOP for professionals to use with children and young people to help keep them safe online.

Childnet International – www.childnet.com/kia
A charity that is helping make the Internet a safe place for children, Childnet International have developed a set of award-winning resources called Know IT All. The resources aim to help educate young people, parents, teachers and volunteers about the safe and positive use of the Internet.

Internet Watch Foundation – www.iwf.org.uk
The IWF is the UK Internet hotline for reporting illegal online content – specifically child sexual abuse images hosted worldwide and criminally obscene and incitement to racial hatred content which is hosted in the UK. The IWF works alongside the government and other such agencies abroad to remove such content from the Internet.

Childline – www.childline.org.uk
Childline is a service provided by the NSPCC offering a free and confidential helpline for children in danger or distress. Children in the UK may call 0800 1111 to talk about any problem 24 hours a day.

UK Council for Child Internet Safety (UKCCIS); http://www.education.gov.uk/ukccis/

UK Safer Internet Centre; http://www.saferinternet.org.uk/