E-Safety Policy

Cranbury College

Development / Monitoring / Review of this Policy

This e-safety policy has been developed in consultation with:

- Headteacher
- Subject Lead for ICT
- Staff – including Teachers, Support Staff, Technical staff
- Management Committee
- PC Solutions (External partner responsible for network service provision)

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the management committee on:	*Insert date*
The implementation of this e-safety policy will be monitored by the:	*e-Safety coordinator – Jaime Scott* *External Provider of Network Management – PC Solutions*
Monitoring will take place at regular intervals:	*Once a year*
The management committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Once a year*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*July 2016*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Insert names / titles of relevant persons / agencies eg: LA ICT Manager, LA Safeguarding Officer, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Reviews of e-safety software provision
- Student Voice
- Staff training and feedback opportunities

E-Safety Policy

Cranbury College

Scope of the Policy

This policy applies to all members of Cranbury College's provision (including staff, students, parents / carers and visitors) who have access to and are users of the College's ICT systems*, both in and outside of the designated premises.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the college's sites.This means that students involved in incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the college, but is linked to membership of the college, can be subject to sanctions and disciplinary action.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Cranbury College will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Cranbury College will deal with e-safety and internet related incidents and behaviour using this policy, and any related policies (such as anti-bullying and safeguarding). Where known, parents / carers will be informed of incidents of inappropriate e-safety behaviour that take place out of school. Where it is deemed necessary, appropriate external agencies (such as the police) will also be informed.

** Staff and visiting employees of RBC should note that this policy does not cover the use of the RBC Northgate system, which has its own procedures and policies which users should be aware of and must follow.*

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within Cranbury College:

Management Committee:

The management committee is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the committee members receiving regular information about e-safety incidents and annual monitoring reports. A member of the management committee has taken on the role of working with the e-Safety coordinator to:

- Review updates to this policy
- Review monitoring systems relating to this policy

Headteacher:

The headteacherhas a duty of care for ensuring the safety (including e-safety) of members of the school community. This includes responsibility for:

- Being aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see RBC flow chart on dealing with e-safety incidents)

- Being aware of the procedures to be followed in the event of a serious e-safety incident that puts a student at risk. (safeguarding)
- Ensuring that at least one other senior leader is also aware of these procedures.
- Ensuring that relevant staff receive suitable training to enable them to carry out their e-safety roles.

e-Safety Coordinator:

The subject lead for ICT at Cranbury College holds responsibility for ICT across the curriculum, and as such becomes the central point of contact for all e-safety queries and concerns. The main responsibilities of this role are:

- Reviewing and monitoring of this policy, including annual feedback to the management committee.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Liaising with the Headteacher and other relevant staff in the event of serious incidents and allegations.
- Liaising with school and external technical staff.
- Centralising reports of e-safety incidents and keeping a log of incidents and concerns to inform future e-safety developments.
- Ensuring that students have access to a Computing curriculum that addresses the National Curriculum programmes of study relating to e-safety and internet use.
- Providing training for staff where necessary, or recommendation of relevant training opportunities for staff to SLT for consideration.

Network Service Provider / Technical Staff:

The network service provider for Cranbury College is responsible for:

- Ensuring that the college's technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensuring that the college meets required e-safety technical requirements and any Local Authority E-Safety Policy / Guidance that may apply.
- Ensuring that users may only access the networks and devices through a properly enforced password protection policy.
- Ensuring that filtering is applied and updated on a regular basis, and that its administration is not the sole responsibility of any single person.
- Keeping up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- Ensuring that the use of the network,internet, Virtual Learning Environment, remote access and email can be monitored in order that any misuse / attempted misuse can be reported to theheadteacher for investigation / action / sanction.
- Ensuring that relevant monitoring software / systems are implemented and updated.

Teaching and Support Staff

are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current college e-safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy.
- They report any suspected misuse or problem to the Headteacher, e-Safety coordinatorand RBC (if appropriate) for investigation / action / sanction.
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other relevant activities.
- Students are aware of and understand the e-safety and acceptable use policies.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc.in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned, students are guided to sites and content checked as suitable for their use and that procedures are followed for dealing with any unsuitable material that is found in internet searches.
- Students have the opportunity to discuss concerns and queries relating to e-safety (and related policies) with staff and their peers through the college Student Voice programme.

Child Protection / Safeguarding Designated Person / Officer

should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students / pupils:

Are responsible for:

- Using the collegeICTsystems in accordance with the Student Acceptable Use Policy.
- Developing an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Engaging in learning which teaches the importance of reporting abuse, misuse or access to inappropriate materials.
- Reporting any concerns they have about e-safety to a member of staff. Students are also expected to bring to staff’s attention access to inappropriate web-based content on the school’s ICT system, whether intentional or not.

- Knowing and understanding policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Understanding that the college's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The college will take every opportunity to help parents understand these issues through progress meetings, letters, website / VLE and information about e-safety campaigns / literature. Parents and carers will be encouraged to support the college in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Their children's personal devices in the college (where this is allowed)
- Access to parents' sections of the website / VLE

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students* to take a responsible approach. The education of *students* in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Education about e-safety should be provided as part of Computing / PHSE / other lessons, and should be regularly revisited and reviewed
- Key e-safety messages should be reinforced as part of the college's programme of assemblies and keyworking activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study.

Education – Parents/ Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, web site
- Student entry interviews and progress meetings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications egwww.swgfl.org.ukwww.saferinternet.org.uk/http://www.childnet.com/parents-and-carers(see appendix for further links / resources)

Education& Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

Cranbury College has a managed ICT service. It is the responsibility of the college to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, as suggested below. The managed service provider should be fully aware of the *college's* E-Safety Policy / Acceptable Use Agreements. The college should also follow Local Authority / other relevant body policies on these technical issues.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

A more detailed Technical Security Template Policy can be found in the appendix.

- Cranbury Collegetechnical systems will be managed in ways that ensure that the college meets recommended technical requirements(these may be outlined in Local Authority / other relevant body policy and guidance)
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to collegetechnical systems and devices.
- All users (at KS2 and above)will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school / academy ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated individual and kept in a secure place.
- Reading Borough Council and Cranbury's DSP areresponsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- School / academy technical staff can monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. (schools may wish to add details of the monitoring programmes that are used).
- An appropriate system is in place (to be described) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- A policy is in place on the system for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- A policy is in place forbids staff without admin rights from downloading executable files and installing programmes on school devices.

Bring Your Own Device (BYOD) *do we remove as not relevant?*

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.(see appendix for a more detailed BYOD Policy Template)

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's / academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students/Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and studentsinstant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet.

Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff and are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Students must not take, use, share, publish or distribute images of others without their permission
- Visitors to Cranbury College sites (including parents / carers) should not take any digital images on site, or of college activities taking place off site, without prior permission. This is due to the high level of vulnerable students catered for by the college. Where permission is granted, images must not be shared or published on the internet.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website. This permission is sought and signed for as part of the admissions paperwork for Cranbury College.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The college must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the Data Protection Act (1998).
- It has a Data Protection Policy(see appendix for template policy do we have one?!)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- It has clear and understood arrangements for the security, storage and transfer of personal data
- There are clear and understood policies and routines for the deletion and disposal of data

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off", or that unsupervised devices are locked, at the end of any session in which they are using personal data.
- Transfer personal data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected.
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

Cranbury College operates from different sites, where student's age groups range from Primary to those who are 18+. As such, different sites set their own rules regarding the acceptable use of communications. These rules are also subject to change in response to student intake, circumstances and learning needs.

Staff are encouraged to recognise that communication technologies can be an effective tool for learning if used responsibly in a safe environment.

Recommended site procedures:

- An up to date copy of the document ‘Accepted Communications’ should be kept in the site e-Safety folder.
- Rules on accepted communications should be communicated clearly to staff and students.
- Students should be involved in feedback regarding changes or review of accepted communications through Student Voice.

Social Media - Protecting Professional Identity

Expectations for teachers’ professional conduct are set out in ‘Teachers Standards 2012’. While, Ofsted’s e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise. Delete this once researched!

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render Cranbury College or the local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues. SWGfL BOOST includes unlimited webinar training on this subject: (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development)
- Clear reporting guidance, including responsibilities, procedures and sanctions

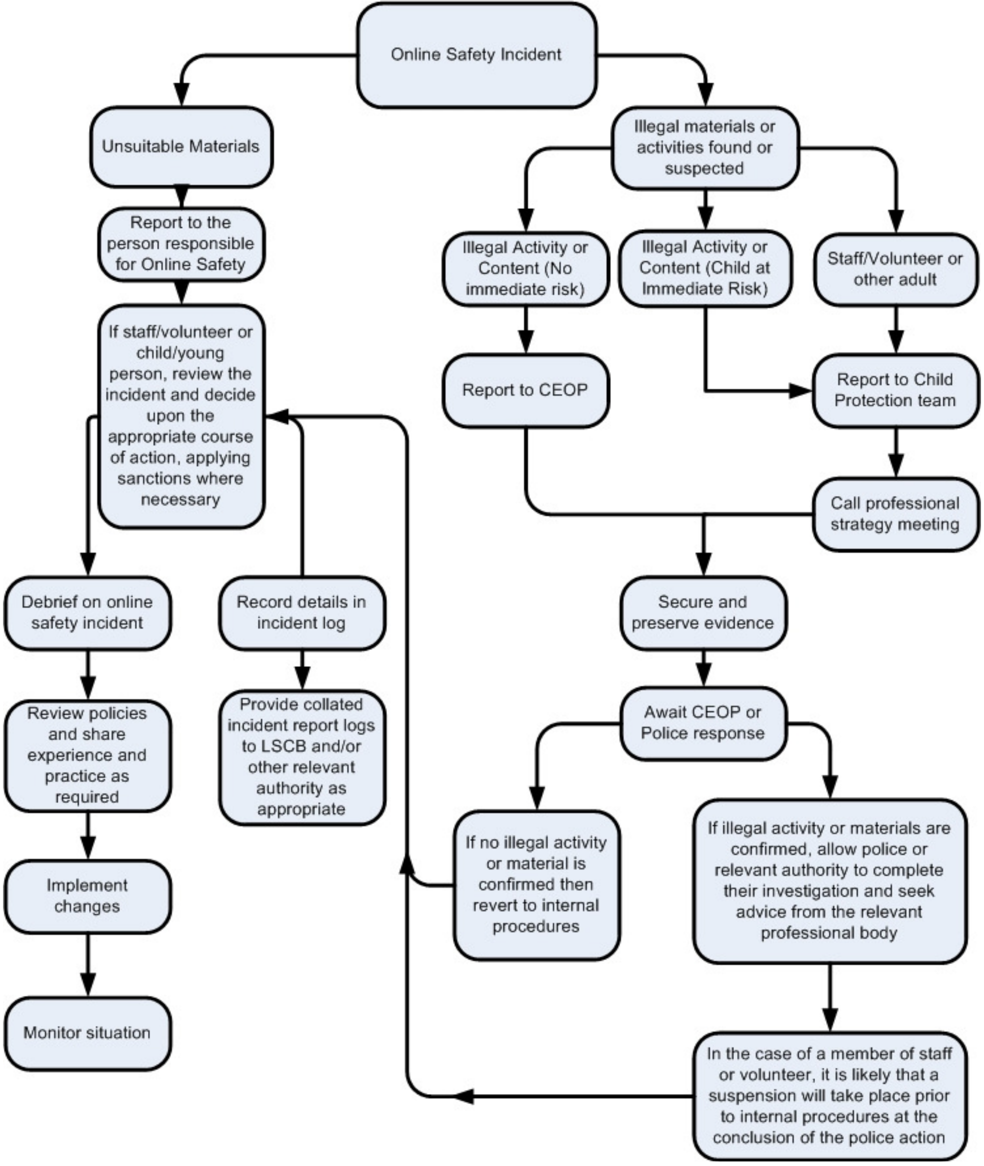
School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to Cranbury College or the local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Any use of social media for professional purposes should be reported to SLT and the e-safety co-ordinator for logging and checking to ensure compliance with the Data Protection policy, acceptable use of communications, and Digital Image and Video agreements.SWGfL BOOST includes SWGfL Alerts that highlight any reference to the school/academy in any online media (newspaper or social media) for example http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Alerts

Illegal Incidents

If there is any suspicion that any web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police. Need to develop own to inc. RBC flowchart referral and reporting to safeguarding officer


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- ***If content being reviewed includes images of Child abusethen the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:***
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- ***Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.***

It is important that all of the above steps are taken as they will provide an evidence trail for the college and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. Any completed forms, notes and paperwork should be retained by the group for evidence and reference purposes.

E-Safety Policy

Cranbury College

School Actions & Sanctions

It is more likely that the college will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

P = Progress sheets CI = Cranbury Incident Sheet IL = Incident Log (Use of Internet) ✓ = Minimum response ✓ = Response dependent on circumstances (see notes) **Incidents:**	Paperwork	Refer to keyworker	Refer to Head of ICT / Lead Teacher / other*	Refer to e-Safety co-ordinator	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights (temp, with review)	Warning (3X warning = further sanction)	Further sanction (proportionate to level of incident, may inc. exclusion)	
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	??			✓	✓	✓		✓	✓		✓	Parents should be informed of any investigations taking place.
Unauthorised use of non-educational sites during lessons	P IL	✓					✓		✓	✓		Removal of access if 3x warnings. If site deemed inappropriate at any time in school (e.g. graphic but legal).
Unauthorised use of mobile phone / digital camera / other mobile device	P CI	✓	✓							✓	✓	Further, appropriate sanction if 3x warning
Unauthorised use of social media / messaging apps / personal email	P	✓	✓				✓			✓	✓	If site deemed inappropriate at any time in school.
Unauthorised downloading or uploading of files	P						✓		✓	✓		Temporary removal of access (set period of time) if 3x warnings.
Allowing others to access school / academy network by sharing username and passwords	P		✓				✓		✓	✓		Technical staff to reset security details of individual(s) involved.
Attempting to access or accessing the school / academy network, using another student's / pupil's account	CI IL	✓	✓				✓	✓	✓		✓	Phone call home as attempted hacking. Technical staff to reset security details of individual(s) involved. Sanction dependent on motive / impact.
Attempting to access or accessing the school / academy network, using the account of a member of staff	CI IL	✓	✓	✓	✓		✓	✓	✓		✓	Phone call home as attempted hacking. Technical staff to reset security details of individual(s) involved. Head / e-Safety coordinator to be informed if staff member allowed unsupervised access.
Corrupting or destroying the data of other users	P CI	✓	✓		✓		✓	✓			✓	Inform technical staff ASAP as recovery of data may be possible.
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	??	✓	✓	✓	✓	✓	✓	✓			✓	Parents should be informed of any investigations taking place.

Recording or photographing staff or students without prior permission	CI ??	✓	✓	✓	✓	✓		✓		✓	✓	Students should promptly comply with allowing a member of staff to check recorded material has been deleted from the device .
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	CI	✓			✓			✓		✓	✓	
Using proxy sites or other means to subvert the school's / academy's filtering system	CI IL		✓				✓			✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	P	✓	✓				✓	✓		✓		
Deliberately accessing or trying to access offensive or pornographic material	CI IL	✓	✓	✓	✓		✓	✓	✓		✓	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	P IL	✓	✓	✓	✓		✓	✓	✓	✓	✓	Examination boards have their own reporting systems for coursework that infringes copyright.

**This referral may simply be to inform planning for adapting the delivery of ICT teaching to cover a current aspect of e-safety, or the delivery of sessions such as PSHE or assembly.*

Removal of access should only ever be temporary, with a review date identified. Length of access restriction will depend on the incident level and circumstances. Before access is reapplied, students should have a review with a suitable member of staff to discuss: a) do they understand why the access was removed and what they need to do to prevent another incident? b) What was the impact on their learning during the period where they didn't have access to the computers?

Parents should be informed if a student's access to computers is withdrawn. This is because it has the potential to impact on learning, and parents must understand why such a decision has been taken and the circumstances leading up to the incident (e.g. warnings given, discussions with keyworkers, teachers etc.).