CHULMLEIGH ACADEMY TRUST

CHULMLEIGH ACADEMY TRUST

ICT POLICY

Including
Password & Security, e-safety, and Acceptable Use Agreements

This policy was adopted by the Board of Directors on: 19.7.18

Information & Communication Technology Policy

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

Vision

ICT within the Academy should be innovative, reliable, embedded within the curriculum and sustainable, allowing students and staff to develop their ICT capabilities in a safe, stimulating and supportive environment.

ICT should build bridges that will overcome distance and link our students and staff to their community and the world around us.

ICT will make a clear contribution to learning and the aims of the college.

Rationale

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

The College has therefore adopted the following aims.

Aims

1. To develop ICT capability: ICT capability involves technical and cognitive proficiency to access, use, develop, create and communicate information appropriately. It requires students and staff to know what ICT is available, when and how to use it and why it is appropriate for the task.
2. To teach students to use the internet safely (e-safety.)
3. To build on the knowledge and skills developed in Key Stage 2 and develop their independence.
4. Provide access to quality ICT resources across all curriculum areas in order to enhance students' learning and to meet their needs and the demands of the Curriculum across all subjects

5. To enable students to become familiar with a range of software and hardware, to gain the confidence to explore new software independently and to give students experience of identification and solution of problems including work on project management
6. To promote educational development including Literacy, Numeracy, Citizenship and encouraging students' thinking skills and to facilitate collaborative learning.
7. To enable students to develop keyboard skills.
8. To provide students with a greater variety of options for expressing ideas in an appropriate and effective manner.
9. To provide suitable learning challenges for all pupils to achieve an ICT qualification.
10. To broaden students' horizons

Scope of the policy

This policy applies to all members of the Academy community (including staff, students / pupils, Directors, volunteers, parents / carers, visitors, community users) who have access to and are users of Academy ICT systems, both in and out of the schools.

Roles and Responsibilities

Executive Headteacher

The Executive Headteacher is responsible for ensuring the safety (including e-safety) of members of the trust, though the day to day responsibility for e-safety will be delegated to the Assistant Headteacher and the Business Manager. The Executive Headteacher is responsible for ensuring that the E-Safety Co-ordinators and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

Assistant Headteacher (e-safety coordinator)

- takes day to day responsibility for e-safety and has a leading role in establishing and reviewing the Academy's ICT and e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaise with the Local Authority
- liaises with Academy ICT technical staff
- meets with Safeguarding Director to discuss issues and review incidents
- Ensures that ICT is covered by all schemes of work
- that he / she keeps 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

□

- Keeps aware of developments in ICT reviews possibilities for their inclusion in the Academy

- Helps colleagues identify their professional development needs in ICT Distributes information about ICT training and development opportunities.

Network Manager / Technical team are responsible for ensuring:

- Working with the strategic ICT provider, manages the Academy computer network and ensure its future development including advising the Executive Headteacher and Directors .
- the ICT budget is managed effectively

- that the Academy's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the Academy meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the Academy's networks through a properly enforced password protection policy, in which passwords are changed in line with Academy policy.
- SWGfL is informed of issues relating to the filtering applied by the Grid
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Assistant Headteacher (e- safety) for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in Academy policies
- Advise on and as needed implement upgrades to system in order to meet the above protocols and those outlined in the technical infrastructure section on page 14.

Curriculum leaders are responsible for:

- ensuring their department's schemes of work provide for the use of ICT to enhance teaching.
- Liaising with the ICT technicians' team to identify hardware and software and how it is to be used. Identifying staff needs for ICT training.

Teaching and Support Staff are responsible for ensuring that:

- they are responsible for the pupil's ICT experiences
- they have an up to date awareness of e-safety matters and of the current Academy esafety policy and practices
- they have read, understood and signed and are following the Academy Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Deputy/Executive Headteacher or Network manager
- that their digital communications with students / pupils are on a professional level *and* only carried out using official Academy systems

- e-safety issues are embedded in all aspects of the curriculum and other Academy activities
- they monitor ICT activity in lessons, extra curricular and extended Academy activities ensuring equipment is used appropriately and safely as defined on page 16
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current Academy policies with regard to these devices.
- students / pupils have a good understanding of research skills, are taught to critically evaluate materials and understand the need to avoid plagiarism and uphold copyright regulations and follow the Academy e-safety and acceptable use policy
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

Senior Designated person for Child Protection

- should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from: (This Designated Person for Child protection is currently also the e-safety officer) ○ sharing of personal data/ access to illegal / inappropriate materials ○ inappropriate on-line contact with adults / strangers ○ potential or actual incidents of grooming ○ cyber-bullying
- should ensure new staff receive information on the Academy's ICT policy and acceptable use agreements.
- Ensure all staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the Academy community (see flowchart on page 11)

Personnel Manager / Administrator in the relevant school

- Will ensure that new staff sign the induction sheet confirming they have completed the induction process that they agree to the ICT acceptable use agreement.
- that all new students, visitors etc will sign a copy of the acceptable use policy

All users within the scope of this policy are responsible for:

- reporting immediately to the Business Manager any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT. This includes lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance.
- ensuring their use of ICT meets that stated in the relevant ICT Acceptable use agreement.
- Complaints and/ or issues relating to eSafety should be made to the Assistant Headteacher or Headteacher.

Policy Review

The policies contained in this document will be reviewed on an annual basis by the ICT and esafety team. This team comprisesthe Assistant Headteacher, , Business Manager and ICT technicians. They will review and advise Directors on any elements of the policies that may need updating. This team will also ensure that the protocols contained within them are being followed and that staff are aware of current guidelines.

Directors will review the ICT policy document every time a change is recommended by the ICT and e-safety team. The Directors will review the document at least every three years even if no changes have been recommended. Directors are responsible for the approval of the E-Safety Policy and for reviewing its effectiveness.

Data Security

The academy holds a variety of sensitive data including personal information about students and staff. If you have been given access to this information, you are reminded of your responsibilities under the General Data Protection Regulations.

You should always be aware of the sensitivity of the information on your computer screen and consider the possibility that those with unauthorised access to this data (other pupils, parents, your family) may be able to see it. This applies when using the academy's systems in school or at home. Screens need to be closed when not being worked on, particularly in the classroom and staff need to be aware of the possibility of sensitive information being shown on classroom whiteboards, for instance SIMS registers and staff email..

You should only take a copy of data outside the academy's systems if absolutely necessary, and you should exhaust all other options before doing so. This includes putting sensitive data onto laptops, memory sticks, cds/dvds or into emails. If you do need to take data outside the academy, you must take all reasonable steps to keep that data secure. As part of this you should perform a risk assessment on the implications of it falling into the wrong hands, and take appropriate steps to mitigate against this. This will almost certainly include encrypting the information, and checking the data protection statements of any recipients of the data.

There are a variety of methods of remote access to systems available (in particular remote desktop such as the U drive or terminal services) which allow you to work on data in-situ rather than taking it outside the Academy, and these should always be used in preference to taking data off-site. The ICT Department offers a variety of information and support to help you keep data secure. If you are uncertain about any aspect of data security, you must contact them for advice.

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" at the end of any session in which they are using personal data.**

- **Transfer data secure password protected devices.** Removable devices must not be used to transfer personal information unless the individual files are password protected. Confidential information must never be transferred on removable devices unless they are encrypted. (eg Sims).

Physical Security

The users of ICT equipment should always adhere to the following guidelines:

- Treat equipment safely, in the same manner as a reasonable person would
- Keep liquids away from ICT equipment
- Do not place heavy objects on ICT equipment
- Do not drop ICT equipment or objects onto it
- Any portable computer or device must be securely locked away when not in use.
- Portable computer and device security is your responsibility at all times.
- Do not leave the portable computer or device unattended in a public place or within the academy
- Do not leave the portable computer or device on view inside your car. It should be locked away in your car's boot out of sight.
- Extra reasonable care must be taken to prevent the loss of USB sticks (which must be encrypted or password protected) which contain confidential academy data
- Staff supervising students using ICT equipment should ensure students take reasonable care of such equipment

When personal data is stored on any portable computer system:

- the data should be password protected (and must as new procedures come into place) be encrypted.
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with trust policy (below) once it has been transferred or its use is complete

Remote Access

Remote connections are considered direct connections to the academy network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Pupils are also issued with Passwords and are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

Staff are aware of their individual responsibilities to protect the security and confidentiality of Academy networks, SIMS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that laptops are not left unattended (unless secured and password protected) and that workstations are locked.

E-safety

The internet is an open communication medium, available to all, at all times. It is an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. **Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.** There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

This section of the policy is supported by the Academy's acceptable use agreements for staff, directors, visitors and pupils. It aims to and educate users about these risks and protect the interests and safety of the whole Academy community. It is linked to the following mandatory Academy policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The Academy will deal with such incidents within this policy and associated acceptable use agreements, 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.

ICT and online resources are increasingly used across the curriculum and whilst regulation and technical solutions are very important we believe the education of students in e-safety is an essential part of the Academy's e-safety provision.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT and PHSE curriculum.
- Key e-safety messages should reinforced in assemblies and tutorial 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be helped to understand the need for the student Acceptable use agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils should be taught to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- All pupils and staff are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to Network manager, ICT technician or teacher as appropriate. The Network manager will then decide if the site should be filtered.
- If a student is found accessing inappropriate material or sending offensive emails the teacher should ask the student to step away from the machine, lock the PC (Alt, Ctr, Del) and immediately contact a technician. If the student refuses to move from the machine the PC should be turned off at the socket (not shut down)as this maintains all logs and web addresses visited
- Staff should act as good role models in their use of ICT, the internet and mobile devices and will receive e-safety training as part of their initial child protection training and their refresher courses.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Headteacher
- Staff and pupils are aware that Academy based email and internet activity can be monitored and explored further if required
- Staff are permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, provided they are transferred immediately and solely to the Academy's network and deleted from staff members device.
- Images taken on any medium (including video conferencing) must never be shared or uploaded to conferencing or social networking sites or other publicly viewable media without the express permission of the parent/carer, pupil and the Headteacher/Marketing manager.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with express permission of the teacher and the pupil, images can be taken provided they are transferred immediately and solely to the Academy's network and deleted from the pupil's device.
- Students must never use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before digital recordings or images of students are published on any public medium. This consent form is considered valid for the entire period that the child attends a school within the Academy. Parents/ carers may withdraw permission, in writing, at any time.

For guidance on the taking using and storing of images please refer to the separate relevant policy

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

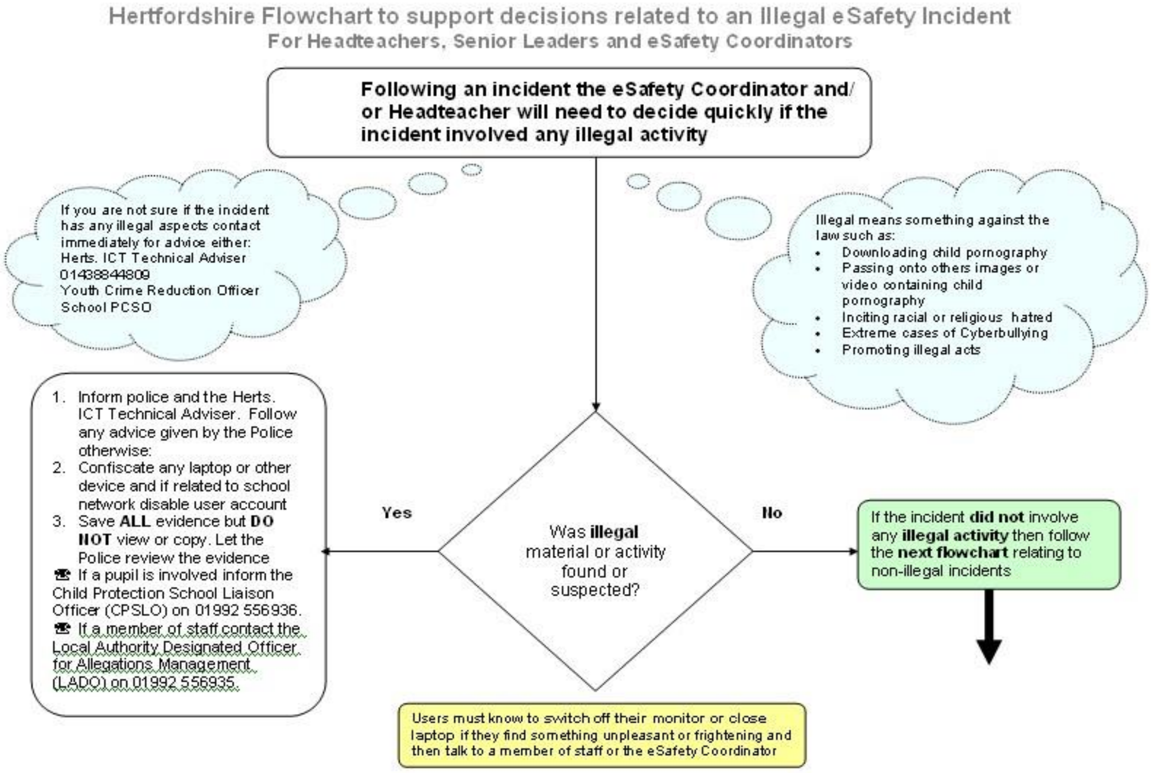
- Websites
- Learning Platforms and VLEs
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/smart phones/tablets
- Other mobile devices with web functionality

Where chat rooms, blogs etc are used as part of the curriculum these will be run from sites specifically designed for schools where security and users have been restricted to those approved by a teacher.

All use of the **Grid for Learning** (SWGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Flow Chart.

The flow charts below has been produced by Hertforshire LA for use by schools in the National grid for learning.



Hertfordshire Flowchart to support decisions related to an Illegal eSafety Incident
For Headteachers, Senior Leaders and eSafety Coordinators

Following an incident the eSafety Coordinator and/ or Headteacher will need to decide quickly if the incident involved any illegal activity

If you are not sure if the incident has any illegal aspects contact immediately for advice either:
Herts. ICT Technical Adviser
01438844809
Youth Crime Reduction Officer
School PCSO

Illegal means something against the law such as:
- Downloading child pornography
- Passing onto others images or video containing child pornography
- Inciting racial or religious hatred
- Extreme cases of Cyberbullying
- Promoting illegal acts

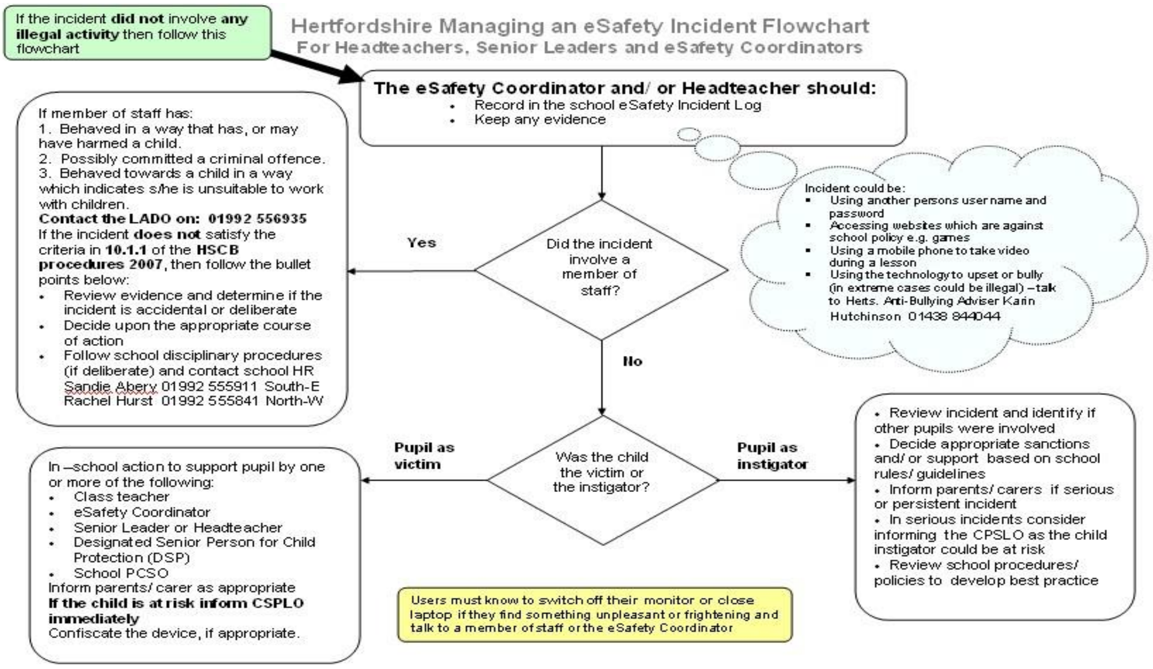
Was **illegal** material or activity found or suspected?

1. Inform police and the Herts. ICT Technical Adviser. Follow any advice given by the Police otherwise:
2. Confiscate any laptop or other device and if related to school network disable user account
3. Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence

☎ If a pupil is involved inform the Child Protection School Liaison Officer (CPSLO) on 01992 556936.
☎ If a member of staff contact the Local Authority Designated Officer for Allegations Management (LADO) on 01992 556935.

If the incident **did not** involve any **illegal activity** then follow the **next flowchart** relating to non-illegal incidents

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator



If the incident **did not** involve **any illegal activity** then follow this flowchart

Hertfordshire Managing an eSafety Incident Flowchart
For Headteachers, Senior Leaders and eSafety Coordinators

The eSafety Coordinator and/ or Headteacher should:

- Record in the school eSafety Incident Log
- Keep any evidence

Incident could be:

- Using another persons user name and password
- Accessing websites which are against school policy e.g. games
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal) – talk to Herts. Anti-Bullying Adviser Karin Hutchinson 01438 844044

Did the incident involve a member of staff?

Yes

If member of staff has:
1. Behaved in a way that has, or may have harmed a child.
2. Possibly committed a criminal offence.
3. Behaved towards a child in a way which indicates s/he is unsuitable to work with children.

Contact the LADO on: 01992 556935

If the incident **does not** satisfy the criteria in **10.1.1** of the **HSCB procedures 2007**, then follow the bullet points below:

- Review evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures (if deliberate) and contact school HR Sandie Abery 01992 555911 South-E Rachel Hurst 01992 555841 North-W

No

Was the child the victim or the instigator?

Pupil as victim

In –school action to support pupil by one or more of the following:

- Class teacher
- eSafety Coordinator
- Senior Leader or Headteacher
- Designated Senior Person for Child Protection (DSP)
- School PCSO

Inform parents/ carer as appropriate
If the child is at risk inform CSPLO immediately
Confiscate the device, if appropriate.

Pupil as instigator

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions and/ or support based on school rules/ guidelines
- Inform parents/ carers if serious or persistent incident
- In serious incidents consider informing the CPSLO as the child instigator could be at risk
- Review school procedures/ policies to develop best practice

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and talk to a member of staff or the eSafety Coordinator

Illegal / Unsuitable / inappropriate activities

The Academy believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using Academy equipment or systems. The Academy policy restricts certain internet usage, a list is provided below for reference but this is not necessarily exhaustive.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: Illegal activities

child sexual abuse images
promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
adult material that potentially breaches the Obscene Publications Act in the UK
criminally racist material in UK
pornography
promotion of any kind of discrimination
promotion of racial or religious hatred
threatening behaviour, including promotion of physical violence or mental harm
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
Using Academy **systems to run a private business**
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
Creating or propagating computer viruses or other harmful files
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet

or Inappropriate activities

Students

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
Unauthorised use of non-educational sites during lessons
Unauthorised use of mobile phone / digital camera / other handheld device
Unauthorised use of social networking / instant messaging / personal email
Unauthorised downloading or uploading of files
Allowing others to access Academy network by sharing username and passwords
Attempting to access or accessing the Academy network, using another student's / pupil's account
Attempting to access or accessing the school network, using the account of a member of staff
Corrupting or destroying the data of other users
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
Continued infringements of the above, following previous warnings or sanctions
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the school
Using proxy sites or other means to subvert the school's filtering system
Accidentally accessing offensive or pornographic material and failing to report the incident
Deliberately accessing or trying to access offensive or pornographic material
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

Staff

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email
Unauthorised downloading or uploading of files
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
Careless use of personal data eg holding or transferring data in an insecure manner

Deliberate actions to breach data protection or network security rules
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils
Actions which could compromise the staff member’s professional standing
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the school
Using proxy sites or other means to subvert the school’s filtering system
Accidentally accessing offensive or pornographic material and failing to report the incident
Deliberately accessing or trying to access offensive or pornographic material
Breaching copyright or licensing regulations
Continued infringements of the above, following previous warnings or sanctions

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on an Academy website)

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the Academy and later in support of their child’s signature. The acceptable use agreement will contain the statement

We will support the school approach to on-line safety and not upload or add any images, sounds or text that could upset or offend any member of the school community

- The Academy disseminates information to parents relating to eSafety where appropriate in the form of;

○ Information and celebration evenings
○ Posters
○ Website/ Learning Platform postings
○ Newsletter items ○ Learning platform training

Technical infrastructure, filtering and monitoring

The Academy will be responsible for ensuring that the Academy infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The procedures below are currently maintained:

- School ICT systems are managed in ways that ensure that the Academy meets the data protection, password and e-safety technical requirements.
- The Academy uses the monitoring solution via the Grid for Learning where web-based activity is monitored and recorded. For further information relating to filtering please go to http://www.thegrid.org.uk/eservices/safety/filtered.shtml
- The responsibility for the management of the Academy's filtering policy will be held by the Network Manager and Senior ICT Technician. They will manage the Academy filtering, in line with this policy .
- Academy ICT technical staff randomly and regularly monitor and log the activity of users on the Academy ICT systems to ensure it is in line with the acceptable use policy.
- Remote management tools are used by staff to control workstations and view users activity
- The Academy infrastructure and individual workstations are protected by up to date virus software
- Polices prevent the downloading and installation of executable files by students
- Staff (other than the ICT team) are not allowed to install software on curriculum or admin computers or laptops without the explicit permission of the Network Manager.
- Pupils and Staff using personal removable media (laptops/tablets/smart phones) are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the Academy's responsibility nor the network manager's to install or maintain virus protection on personal systems.
- If pupils or staff wish to bring in work on removable media it must be given to the ICT technicians for a safety check first.
- Images/ films of children are stored on the Academy's network Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform

- The Academy uses CCTV for security and safety. The only people with access to this are **the ICT and Estates teams, SLT and on occasion other senior middle leaders who have gained permission from a member of SLT.** Notification of CCTV use is displayed at each locations where CCTV is used. Please refer to the hyperlink below for further guidance http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx

- Webcams are also used in ICT suites for education purposes. Their use is covered by the digital images elements in the acceptable use agreement.

- There are regular reviews and audits of the safety and security of Academy ICT systems. These take place at team meetings, meetings with the Line manager and Deputy Executive Headteacher

- Main Servers and back devices are securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the Academy systems and data.
- All users have clearly defined access rights to Academy ICT systems. users can only access data to which they have right of access
- All users at KS2 and above are provided with a username and password. These are only be provided to staff or student teachers after relevant CRB checks have been satisfied.
- The provision of temporary access of "guests" onto the Academy system is on the basis of restricted access
- Passwords shall not be displayed on screen, and shall be securely hashed
- Staff laptops must be password protected (and must as new procedures come into place) be encrypted.
- The "master / administrator" password for the Academy ICT system are kept in the school safe. The network manager/ senior technicians and Deputy Executive Headteacher (strategic ICT and e-safety) also have passwords with administrative rights.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

ICT in the Curriculum

ICT expands horizons by shrinking worlds (David Brown)

ICT should offer opportunities of pupils to:

- Prepare themselves for participation in a rapidly changing world where activities are increasingly transformed by access to ICT.
- Develop initiative, confidence and independent learning skills.

- Gain rapid access to ideas and experiences from a wide range of people, communities and cultures relevant to the subject (and more widely)
- Support the pedagogy of the subject and help develop and sustain learning and broaden students horizons
- develop a critical awareness of the effects of ICT on individuals and societies Acquire knowledge and understanding of how ICT can help their work in other subjects.
- know about the nature and variety of ICT equipment and software tools and become skilled in the use of ICT for a variety of tasks

Resources:

Pupils should have access to:

- A computer system that is less than 5 years old
- A range of software and peripheral resources that gives them full access to Curriculum requirements
- Computer systems that are deployed effectively for teaching and learning ICT
- Computer facilities that meet health and safety requirements Computer systems that have high speed links to the Internet and Email All teaching rooms should have Interactive whiteboards and projectors.

Use of ICT suites

ICT is a valuable resource within the college and as such it is everyone's responsibility to ensure that it is used safely and cared for in an appropriate manner therefore:

- Students are not allowed at eat or drink in an ICT suite (if they require water they need to stand by the door.)
- Students are not allowed to touch the back of computer under any circumstances. (If you feel a wire may be loose the teacher may check it or call a technician)
- Students are not allowed to unplug wires to plug in their own equipment. (There are empty USB slots on all the computers so there is no need to do this).
- If as a teacher you unplug a wire –e.g. a power or network socket at parents evening, or a network wire/interactive whiteboard lead during a lesson, you must ensure it is plugged back in when you have finished. This means the room and equipment are ready for your colleagues to use.
- Students and staff should proof read and print preview all documents before allowing them to go to print.
- At the end of a session the ICT suite should be left **as you would expect to leave your own classroom**. Chairs should be under desks and the work space should be tidy

(keyboards, monitors and mice straight, Headphones on the back of monitors and webcams on top of monitor) and the floor area clean.

- Any damage must be reported to the ICT technicians before leaving the room.

Use of Internet in Education Risk assessment.

Risk	Explanation	Solution
Exposure to inappropriate materials	Material that is pornographic, hateful or violent in nature or encourages activities that are dangerous or illegal	SWGFL filtered internet access, good classroom supervision, all staff made aware of risk.
Inappropriate or illegal behaviour	Just as in the real world young people may get involved inappropriate, antisocial or illegal behaviour while using new technologies. For example on line bullying	Appropriate time is provided within the curriculum to teach about internet safety. Students are aware of the internet safety rules.
Copyright infringement	This could include downloading copyrighted materials such as music files, or copying others homework	Appropriate time is provided within the curriculum to teach about internet safety. Students are aware of the internet safety rules.
Obsessive use of the internet and ICT	This could lead to a deterioration in the quality of schoolwork or a negative impact upon family relationships	Appropriate time is provided within the curriculum to teach about the appropriate use of ICT
Physical danger and sexual abuse	This would include paedophiles using internet chat rooms to target and develop relationships with young people for the sole purpose of sexual activity	Appropriate time is provided within the curriculum to teach about internet safety. Students are aware of the internet safety rules.
Inappropriate or illegal behaviour by school staff	This could include viewing or circulating inappropriate material	Staff aware of acceptable use policy.

Current Legislation

Acts Relating to Monitoring of Staff eMail

General Data Protection Regulations 2018

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

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

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

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

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

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

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 – 3)

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

- access to computer files or software without permission (for example using another 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 (section 1)

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

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining 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)

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

Protection of Children Act 1978 (Section 1)

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

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

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

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

Acts Relating to the Protection of Personal Data *Data Protection*

Act 1998 http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

(Soon to be updated to the Data Protection Act 2018)

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.asp

x

Primary Pupil Acceptable Use Agreement

Dear Parent(s)/Carer(s)

ICT, including the internet, e-mail and mobile technologies, etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT. Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact: Linda Lindley (CPS/BPS) and Angela Joslin/Tracey Dodd (EWPS/LPS).

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only use my own username and password and not anyone else's.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- If I see anything I'm unhappy with or receive any emails I don't like, I will tell a teacher.

- I will never use someone else’s photo.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will be aware of “stranger danger” when I am online.
- I will tell a teacher if I accidentally damage a computer or if I see someone else do so.
- When I am using the internet to find information, I will remember that the information I find may not be truthful.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I will only use my memory stick if I have permission from a teacher.
- I will not install any new programs on the computer or change any settings.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my eSafety.

Primary Acceptable Use Agreement: Reply slip

Pupil and Parent/Carer signature

I/We have discussed this ICT acceptable use agreement and

…………………………………………......... (pupil name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at the schools within Chulmleigh Academy Trust.

I/We understand that the Academy will take every reasonable precaution to ensure that young people will stay safe on the internet and this includes providing e-safety information, monitoring use and filtering internet access. However the Academy cannot ultimately be responsible for the nature and content of materials accessed on the internet and using mobile technologies.

Child's name ……………………………………………………………………………….

Child's signature (if appropriate) ……………………………………………… Class

…………………………………….... Date ………………………………..

Primary School………………………………………………………………………….

Parent/ Carer Signature …….……………………..……………………………….

Date ………………………………..

Secondary Acceptable Use Agreement

Dear Parent/Carer and Student

ICT including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school. It is essential that all students are safe and responsible when using any ICT. Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or Mrs Stabb.

Please return the attached section of this form to the College for filing.

- I will only use Academy ICT systems, including the internet, e-mail, digital video, mobile technologies, etc. for learning purposes.
- I will not download or install software on Academy equipment.
- I will only log on to the school network/Learning Platform with my own user name and password.
- I will not reveal my passwords to anyone and will change them regularly.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I understand that the sending of inappropriate email or text messages between any member of the Academy community is not allowed.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring it into disrepute.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material (including images, video, sounds or text) that could be considered offensive or illegal or that upset or offend any member of the school community. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not attempt to bypass the school internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of pupils and/or staff I have taken in school or in relation to a college activity will only be stored and used for school purposes in line with school policy. They will not be distributed outside the school network without written permission from the person in the image and the school.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions may be applied and my parent/carer may be contacted.

Secondary Acceptable Use Agreement: Reply slip

Student and Parent/Carer signature

I/ We have discussed this ICT acceptable use agreement and

…………………………………..................(student name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at Chulmleigh Community College.

We understand that the school will take every reasonable precaution to ensure that young people will stay safe on the internet and this includes providing e-safety information, monitoring use and filtering internet access. However the school cannot ultimately be responsible for the nature and content of materials access on the internet and using mobile technologies.

Parent/Carer Signature …….…………………..……………………………….

Student Signature……………………………………………………………….

Date ………………………………

Tutor group ………………………………….

Year group……………………………………

Staff, Director, Visitor

Acceptable Use Agreement and code of conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Deputy Executive Headteacher (ICT)

- I will only use the Academy's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Executive Head Teacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the Academy or other related authorities
- I will ensure my computer is shutdown, logged off or locked when not in use. I will not leave my laptop or other device unattended unless it is secure.
- I will not give out my own personal details, such as personal e-mail address, to pupils.
- I will only communicate with student's pupils and parents using the official Academy systems. Any such communication with be in a professional tone and manner.
- When communicating with colleagues I will not use aggressive or inappropriate language and I appreciate that others may have a difference of opinion
- I understand that the data protection policy requires that any staff or pupil data/ information which I have access to is kept private and confidential, except when it is deemed necessary that I am required by law or by Academy policy to disclose such information to an appropriate authority.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. I will report any breaches immediately.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with Academy policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the Academy network without the permission of the parent/ carer, member of staff or Headteacher. If images are taken any personal devices they will be transferred immediately and solely to the Academy system and the original deleted (no recycle bin)
- I will ensure that my data is backed up regularly.
- I will not install any hardware of software without permission of the network manager
- I will not disable or cause damage to Academy equipment or the equipment belonging to others
- I will supervise student use of ICT suites as outlined in this policy and in the staff handbook
- I understand that the use of any personal equipment used in school or for school purposes is covered by the ICT policy and I will use it in accordance with this agreement in the same way I would Academy equipment.

- Any personal equipment I use in school must not be connected to the Academy network without the express permission of the Network manager or Senior ICT technician
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will immediately report to the Network manager any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT. This includes lost/stolen equipment or data (including passwords and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy noncompliance.
- I will support the Academy approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the Academy community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will not make students a “friend” on personal Social networking sites and will be cautious about making ex-students friends if they have younger siblings at the Academy.
- I understand that, as I am a person in a position of trust, students are classified as children until they reach the age of 18.
- I will support and promote the Academy’s e-Safety and Data Protection policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I understand that this acceptable use agreement applies not only to my use of Academy ICT equipment but also applies to my use of Academy ICT systems and equipment out of school, and to my personal in equipment in school or when being used in relation to my Academy employment.

I understand that if I fail to comply with the acceptable use agreement I could be subject to disciplinary action. This could include a warning, a suspension, referral to Directors and in the event of illegal activities the involvement of the police.

I agree to follow this acceptable use agreement and to support the safe and secure use of ICT throughout the Academy

Signature ………………………………… Date ……………………

Full Name ………………………………...(printed)

Please note

Staff signatures will obtained and recorded as part of the induction Child Protection Training and at the refresher courses.