E-SAFETY ADVICE AND GUIDANCE

Rationale

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

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

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and instant messaging
- Chat rooms and social networking
- Blogs and Wikis
- Podcasting
- Video broadcasting
- Music download
- Gaming
- Mobile/Smart phones with text, video and web functionality
- Other mobile devices with web functionality

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

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

This policy and acceptable use agreement (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet technologies provided by the school – PCs, laptops, tablets, whiteboards, digital video equipment, etc; and technologies owned by students and staff, but brought onto school premises – laptops, mobile phones, camera phones, and portable media players.

The requirement to ensure that children and young people are able to use the internet and related communication technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school E-Safety policy should help to ensure safe and appropriate use. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

Scope

This guidance applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. This policy should be reviewed in line with the School Information Security Policy.

Monitoring and Review of the E-Safety Policy:

This E-Safety policy has been developed by SLT.

The views of the school community have been sought by the E-Safety group which includes:

Mr K Archer	Governor (New Technologies)
Mr S Ball	Governor (Responsible for E-Safety)
Mr B Warren	Headteacher
Mr M Boucher	Assistant Headteacher
Mrs J Robinson	Assistant Headteacher
Mr A Dixon	Head of ICT
Representative students from each year group	

The SLT will monitor the impact of the policy using**:**

- Logs of reported incidents
- DGfL internal monitoring logs of internet activity (including sites visited)
- Internal monitoring of data for network activity
- Surveys / questionnaires of stakeholders

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governor with responsibility for E-Safety (Mr S Ball) and the E-Safety co-ordinators (Mr Boucher and Mrs Robinson) who will report on a termly basis to the Headteacher who will include an update for the governing body in the termly Headteachers' Report to Governors.

The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Co-ordinators
- Receive monitoring of E-Safety incident logs
- Receive monitoring reports of the filtering of web sites
- Feedback to the full governing body at their termly meeting.

Headteacher

The Headteacher is responsible for ensuring the safety (including E-Safety) of members of the school community and is the school's Senior Information Risk Owner (SIRO). The school's SIRO is responsible for reporting security incidents as outlined in the school's Information Security Policy. The day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinators

- The Headteacher is responsible for ensuring that the E-Safety Coordinators and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues as relevant. E-safety Co-ordinators are also responsible for ensuring that students are taught how to use ICT tools such as the internet, email and social networking sites, safely and appropriately

- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles-

  (The LA has produced guidance relating to the reporting procedure for E Safety incidents- see appendix 1)

- The Headteacher and another member of the SLT should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff-

  (*The LA has produced guidance relating to the reporting procedure for E Safety incidents- see appendix 1)*

- The Headteacher is responsible for ensuring that parents and carers, when given access to data and information relating to their child/children have adequate information and guidance relating to the safe and appropriate use of the online facility-

  (The Information Security Policy contains detailed guidance)

E-Safety Coordinator/Officer:

The school has named persons (Mr Boucher and Mrs Robinson) with the day to day responsibilities for E-Safety. Responsibilities include:

- Leading the E-Safety committee
- Taking day to day responsibility for E-Safety issues and having a leading role in establishing and reviewing the school E-Safety policies / documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Providing training and advice for staff
- Liaising with the Local Authority
- Liaising with the school's SIRO to ensure all school data and information is kept safe and secure
- Liaising with school ICT technical staff and/or school contact from the managed service provider- RM

- Receiving reports of E-Safety incidents and creating a log of incidents to inform future E-Safety developments
- Meeting regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering
- Attending relevant meetings / Governor committee meetings
- Reporting regularly to Senior Leadership Team

Managed service provider:

The managed service provider is responsible for helping the school to ensure that it meets the E-Safety technical requirements outlined by DGfL. The managed service provides a number of tools to schools including; Smartcache servers, Securus NG, SafetyNet Universal and Anti-Virus , which are designed to help schools keep users safe when on-line in school
(see appendix 2).

Schools are able to configure many of these locally or can choose to keep standard settings.

The DGfL Client team work with school representatives to develop and update a range of Acceptable Use Policies *(see Appendix 3)* and any relevant Local Authority E-Safety policy and guidance.

Members of the DGfL team will support schools to improve their E-Safety strategy
The managed service provider maintains backups of email traffic for 90 days. If access to this information is required, the school should contact the DGfL team.

Staff:

Are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the E-Safety Co-ordinators for investigation / action / sanction.
- Digital communications with students eg email, FROG 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 school activities
- Students understand and follow the school E-Safety and acceptable use policy and they encourage students to develop good habits when using ICT to keep themselves safe.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- 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 school policies with regard to these devices (see D38 Guidance for Safer Working Practice for Adults who Work with Children and Young People (Dec 2013) – STIF 5.4

- In lessons where internet use is pre-planned, students are 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. They include the teaching of E-Safety in their lessons

Designated person for Child Protection / Child Protection Officer:

The named Child Protection Officer is Julie Robinson.
The named person is trained in E-Safety issues and is aware of the potential for serious child protection 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

E-Safety Committee:

Members of the E-Safety committee will assist the E-Safety Coordinators with:

- Review of the school E-Safety policy / documents
- Review of the managed service (see Appendix 4 – School's filtering policy)

Students:

Students have access to the school network and technologies that enable them to communicate with others beyond the school environment. The network is a secure and safe system provided through DGfL. Students:

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy *(see appendix 3*), which they will be expected to agree to before being given access to school systems .
- Need to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images, use of social networking sites and on cyber-bullying
- Should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety policy covers their actions out of school, if related to the use of an externally available web-based system provided by 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 school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website.

Community Users/'Guest Access':

Community Users who access school ICT systems and Learning Platform as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems-see appendix 3.

Policy Statement

Education – students

There is a planned and progressive E-Safety/E-literacy curriculum. Learning opportunities are embedded into the curriculum throughout the school and are taught in all year groups.
E-Safety education is provided in the following ways:

- The School has a framework for teaching internet skills in ICT lessons. These are integrated into the Key Stage 3:

    - Year 7 Unit 7.1 – E-Safety

  These are integrated into the Key Stage 4 curriculum

    - GCSE Computing

- Educating students on the dangers of technologies that maybe encountered outside school is done when opportunities arise and as part of the E-Safety curriculum including assemblies and enrichment days.

- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

- Students are taught about copyright and respecting other people's information, images etc through discussion, modelling and activities.

- Students are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; ie parent, carer, teacher, online bullying-box, trusted staff member, or an organisation such as Childline / CEOP report abuse button.

- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

- Students are taught the importance of information security and the need to keep information such as their password safe and secure

- Staff act as good role models in their use of ICT, the internet and mobile devices

Education – parents/carers

The school provides information and awareness to parents and carers through:

- Letters, newsletters, and school's website
- Parents' evenings

Education & Training – Staff

All staff receive regular E-Safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- All new staff receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies. (see D38 Guidance for Safer Working Practice for Adults who Work with Children and Young People (Dec 2013) – STIF 5.4)

- Formal E-Safety training is made available to staff. Staff are reminded / updated about E-Safety matters at least once a year.

- Where staff identify E-Safety as a training need within the performance management/development review process this will be treated as a priority for professional development.

- The E-Safety Coordinators receive regular updates through attendance at DGfL/LA/other information/training sessions and by reviewing guidance documents released by DfE DGfL/LA and others.

- The E-Safety Coordinators provide advice/guidance/training as required to individuals

- This E-Safety policy and its updates are presented to and discussed by staff in staff/team meeting/training days.

All staff are familiar with the school's Policy including:

- Safe use of e-mail
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social networking
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as iPads, mobile phones and digital cameras
- Publication of student information/photographs and use of website
- Cyberbullying procedures
- Their role in providing E-Safety education for students
- The need to keep personal information secure

Training – Governors

Governors take part in E-Safety training / awareness sessions, particularly those with named responsibility ICT / E-Safety / health and safety / child protection

This is offered by:

- Attendance at training provided by the Local Authority / National Governors Association / DGfL or other relevant organisation
- Participation in school training / information sessions for staff or parents
- Regular agenda item for full governors.

Technical – infrastructure / equipment, filtering and monitoring

The managed service provider is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible. The school is responsible for ensuring that policies and procedures approved within this policy are implemented.

School ICT systems will be managed in ways that ensure that the school meets the E-Safety technical requirements outlined in the Acceptable Use Policies

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

All users will have clearly defined access rights to school ICT systems

- All users will be provided with a username and password
- Staff will be required to change their password every 90 days through the use of Password Plus
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school maintains and supports the managed filtering service provided by DGfL
- The school can provide enhanced user-level filtering through the use of the Smoothwall
- The school manages and updates filtering issues through the RM helpdesk and by direct manipulation of Smoothwall

- Requests from staff for sites to be removed from the filtered list will be considered by the E-Safety co-ordinators in consultation with the Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee
- Remote management tools are used by staff to control students workstations and view users activity eg RM Tutor
- An appropriate system is in place for users to report any actual / potential E-Safety incident to the relevant person
- The managed service provider ensures that 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 school systems and data eg Anti-Virus protection
- An agreed procedure is in place for the provision of temporary access to “guests” (eg trainee teachers, visitors) onto the school system
- Only staff with privileged user access can download executable files
- An agreed procedure is in place regarding the extent of personal use that users (staff / students / students / community users) and their family members are allowed on laptops and other portable devices that may be used out of school (see Appendix 5 - ICT Loan Document)
- An agreed procedure is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices (See Information Security Policy)
- The school infrastructure and individual workstations are protected by up to date virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

Curriculum

E-Safety is a focus in all areas of the curriculum and staff re-enforce E-Safety messages in the use of ICT across the curriculum.

- In lessons, where internet use is pre-planned, students are guided to sites checked as suitable for their use and there are processes in place for dealing with any unsuitable material that is found in internet searches *(*The school offers the use of ICE, a search engine, to ensure students’ access to the web is safe).
- Where students are allowed to freely search the internet, eg using search engines, staff should monitor the content of the websites the young people visit
- The school provides opportunities within a range of curriculum areas to teach about E-Safety
- 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 Network Manager or managed service provider temporarily remove those sites from the filtered list for the period of study. Any requests to do so are auditable and should be logged
- Students are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying.

- Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, Child Protection Team or an organisation such as Childline or CEOP report abuse button.

Use of digital and video images

When using digital images, staff inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They recognise the risks attached to publishing their own images on the internet eg on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, and follow school policies concerning the sharing, distribution and publication of those images. Those images are only taken on school equipment, the personal equipment of staff is not used for such purposes
- Care is taken when capturing digital / video images, ensuring students are appropriately dressed and that they are not participating in activities that might bring the individuals or the school into disrepute
- Students must not take, 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 comply with good practice guidance on the use of such images
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers is obtained before photographs of students are published. Permission is also sought from students in KS4.

Data Protection

Personal data is 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.

Staff are aware of the Dudley Information Security Policy. A breach of the Data Protection Act may result in the school or an individual fine of up to £500000

Handling Personal Data

- Ensure that all reasonable care and attention is taken to keep personal data safe and to minimise the risk of its loss or misuse.
- Personal data should be accessed on secure password protected computers and other devices ensuring that they are properly 'logged off' at the end of any session involving the use of personal data.

Before any personal data is saved for use outside the school authorisation should be obtained from the Headteacher. If personal data is stored on any portable computer system or USB stick or any other removable media:

- Data **must** be encrypted and password protected
- 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 school policy once transfer has been completed.

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems eg by remote access from home- *(If staff use non standard or personal email accounts these are not secure and cannot always be monitored)*
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications
- Students are provided with individual school email addresses for educational use
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff
- Students are allowed to bring personal mobile devices/phones to school but must not use them within the building during the school day except when specifically given permission for a particular learning activity.
- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a student or parent/ carer using their personal device unless authorised to do so by the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device
- The school provides a safe and secure way of using chat rooms, blogs and other ‘social networking technologies’ via FROG. Other ‘social networking’ facilities may be ‘unfiltered’ for curriculum purposes. Staff are aware of the procedure they need to follow when requesting access to externally based social networking sites

Unsuitable / inappropriate activities

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

The school will take all reasonable precautions to ensure E-Safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

- Staff and students are given information about infringements in use and possible sanctions. Student sanctions are listed in the Code of Conduct. (see D38 Guidance for Safer Working Practice for Adults who Work with Children and Young People (Dec 2013) – STIF 5.4)

The LA has set out the reporting procedure for E-Safety incidents (see Appendix 1).

Our E-Safety Coordinators act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Governor with responsibility for E-Safety is: Steve Bull

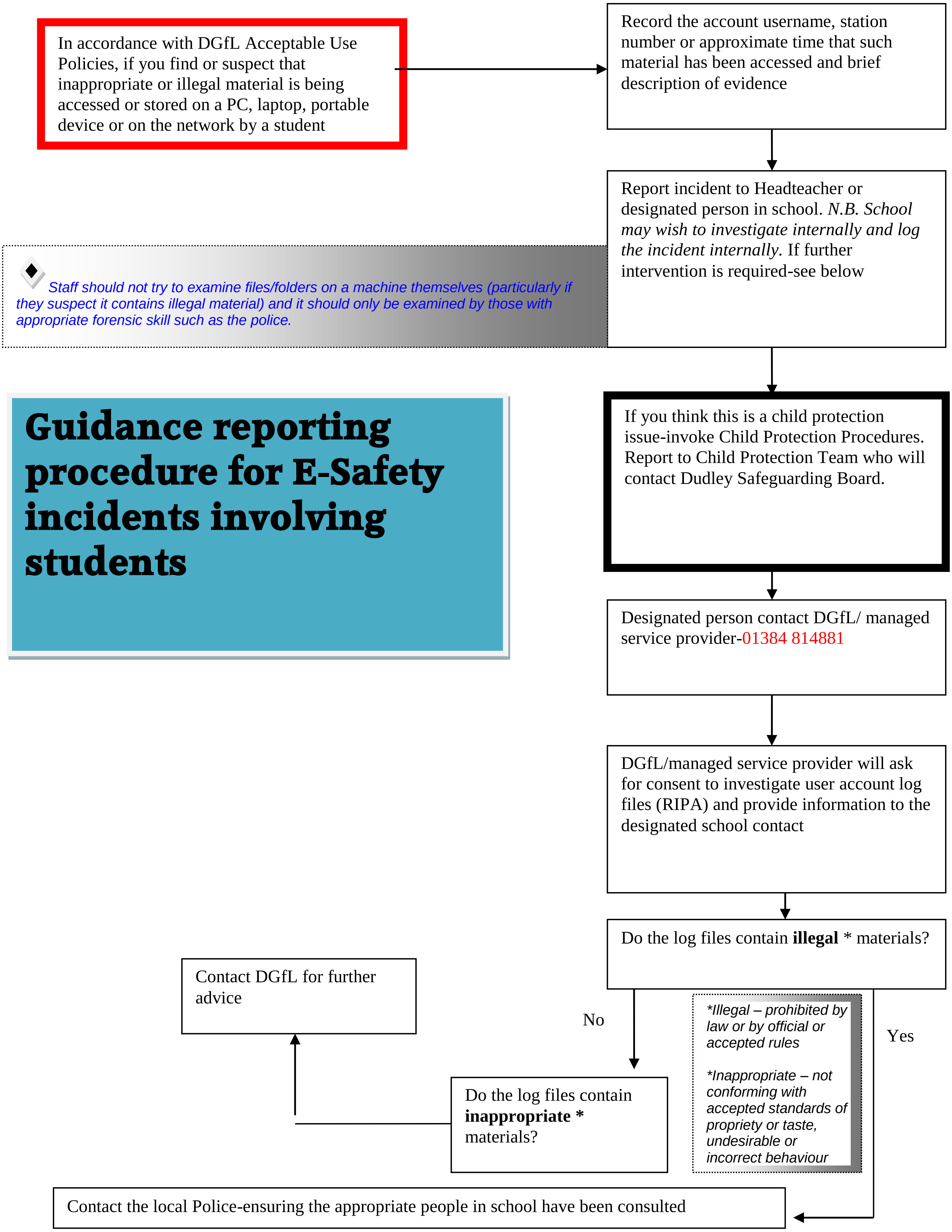
Date the Policy was approved by Governors: 18 October 2011

Date for review July 2016

This E-Safety Guidance and Policy has been written with references to the following sources of information:

BECTA
Dudley LA
Hertfordshire E-Safety Policy
Kent E-Safety Policies, Information and Guidance
South West Grid For Learning- School E-Safety Policy

Appendix 1 -Guidance procedure for E-Safety incidents



In accordance with DGfL Acceptable Use Policies, if you find or suspect that inappropriate or illegal material is being accessed or stored on a PC, laptop, portable device or on the network by a student

Record the account username, station number or approximate time that such material has been accessed and brief description of evidence

Report incident to Headteacher or designated person in school. *N.B. School may wish to investigate internally and log the incident internally*. If further intervention is required-see below

◆ *Staff should not try to examine files/folders on a machine themselves (particularly if they suspect it contains illegal material) and it should only be examined by those with appropriate forensic skill such as the police.*

Guidance reporting procedure for E-Safety incidents involving students

If you think this is a child protection issue-invoke Child Protection Procedures. Report to Child Protection Team who will contact Dudley Safeguarding Board.

Designated person contact DGfL/ managed service provider-01384 814881

DGfL/managed service provider will ask for consent to investigate user account log files (RIPA) and provide information to the designated school contact

Do the log files contain **illegal** * materials?

No

Do the log files contain **inappropriate *** materials?

Contact DGfL for further advice

Yes

Contact the local Police-ensuring the appropriate people in school have been consulted

**Illegal – prohibited by law or by official or accepted rules*

**Inappropriate – not conforming with accepted standards of propriety or taste, undesirable or incorrect behaviour*

Appendix 2-E-Safety tools available on the DGfL network

E-Safety tool	Type	Availability	Where	Details
Smoothwall/ SafetyNet Universal	Web filtering	Provided as part of DGfL	All network connected devices within DGfL	Gives schools the ability to audit, filter and un-filter websites
RM Tutor	Teacher support	Provided as part of DGfL	Managed school desktops	Allows teachers to view and demonstrate screens, control hardware and distribute work
CC4 AUP	Awareness raising	Part of CC4-needs to be enabled	All CC4 stations at log in	When enabled through the management console, users are given an acceptable use policy at log in
Securus NG	Monitoring software	Available to all schools who sign an agreement and attend training	All school XP desktops and networked laptops	Takes a snapshot of a screen when an event is triggered. A range of events can be monitored
Email	Filtering and list control	Provided as part of DGfL	Office 365 Outlook	Allows schools to restrict where email is sent from/to
RM Password Plus	Safe practice	Provided as part of DGfL3	All CC4 stations	A password management tool that enforces password rules of complexity and length for different users

Appendix 3

Summerhill School
Rules for Responsible Computer and Internet Use for Students

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others. It is important that you read this policy carefully. If there is anything that you do not understand, please ask.
I agree that:

- I will not share my password with anyone, or use anyone else's password. If I become aware of another individual's password, I will inform that person and a member of the school staff.
- I will use a 'strong' password ie one that contains letters (upper case and lower case), numbers and possibly symbols which I will change on a regular basis.
- I will use school equipment properly and not interfere with the work or data of another student.
- I understand that the school may check my computer files and may monitor the internet sites I visit.
- Before I use or connect my own equipment (mobile phone, ipod, non-school laptop/tablet etc) I will check with a member of staff to see if that is allowed.
- If I connect a storage device eg flash drive, CDs or DVD, ipod to the school computer I understand that I must make sure that every file on it is appropriate for the school environment and school may check this.
- If I use a flash drive or other storage device eg CDs/DVDs, I will follow school guidelines and use them appropriately.
- I am responsible for all e-mail, chat, sms blogs etc that I post or send and will use language appropriate to the audience who may read them. I will be respectful in how I talk to and work with others online and never write or participate in online bullying. I will report any unpleasant material or messages sent to me. I understand my report will be confidential and may help protect other students and myself.
- I know that posting anonymous messages and forwarding chain letters is not allowed.
- Any files attached to an email will be appropriate to the body of the email and not include any inappropriate materials or anything that threatens the integrity of the school ICT system.
- I will not download or bring into school unauthorised programmes, including games and music, or run them on school computers, netbooks or laptops.
- I will not access inappropriate materials such as pornographic, racist or offensive material or use the school system for personal financial gain, gambling, political purposes or advertising.
- When using the internet including a 'chat room' facility, I will not give my home address or telephone/mobile number, respond to requests using SMS or even arrange to meet someone.
- I will always follow the 'terms and conditions' when using a site. I know content on the web is someone's property and I will ask a responsible adult if I want to use information, pictures, video, music or sound to ensure I do not break copyright law.
- I will think carefully about what I read on the internet, question if it is from a reliable source before I use the information, crediting the source.
- I will not take photographs or make audio or video recordings of another student or another person without his/her permission.

- I will always check with a responsible adult before I share or publish created content of myself or others.

I am aware of the CEOP report button and know when to use it.

CEOP REPORT
ceop.police.uk

I know that anything I share online may be monitored.
I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Appendix 3

Summerhill School
Staff Acceptable Use Policy
Rules for Responsible Computer and Internet use

This policy applies to all adult users of the schools systems. We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Headteacher or your line manager.
Any inappropriate use of the School's internet and email systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal. Electronic information can be produced in court in the same way as oral or written statements.

Research Machines (RM) has a contractual obligation to monitor the use of the internet and email services provided as part of DGfL, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to view, send and receive electronic communications or to access the internet.

All information relating to our students, parents and staff is personal. You must treat all school information with the utmost care whether held on paper or electronically.

Staff will not share passwords with anyone, or use anyone else's password. If a staff member becomes aware of another individual's password, they should inform that person immediately or a member of SLT

All staff must use a 'strong' password ie one that contains letters (upper case and lower case), numbers and possibly symbols which must be changed on a regular basis.

Official school systems must be used at all times.

Use of the internet and intranet

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply:-

- If you download any image, text or material check if it is copyright protected. If it is then follow the school procedure for using copyright material. (Details published by photocopy machines)
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to the Headteacher.
- If you want to download any software, first seek permission from the Headteacher and/or member of staff responsible /RM. They should check that the source is safe and appropriately licensed.
- If you are involved in creating, amending or deleting web pages or content on the website, such actions should be consistent with your responsibilities and be in the best interests of the School.
- You should not :
    - introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
    - seek to gain access to restricted areas of the network;
    - knowingly seek to access data which you are not authorised to view;
    - introduce any form of computer viruses;
    - carry out other hacking activities.

Electronic Mail

Care must be taken when using email as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school.

Internet and email access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your Headteacher. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the school's business purposes which include the following:

1. providing evidence of business transactions;
2. making sure the school's business procedures are adhered to;
3. training and monitoring standards of service;
4. preventing or detecting unauthorised use of the communications systems or criminal activities;
5. maintaining the effective operation of communication systems.

In line with this policy the following statements apply:-

- You should agree with recipients that the use of email is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using email or amend any messages received.
- Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or

incitement to racial hatred in the same way as making such comments verbally or in writing.
- It is good practice to re-read email before sending them as external email cannot be retrieved once they have been sent.
- If the email is personal, it is good practice to use the word ‘personal’ in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.
- Internet and email access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your Headteacher.
- All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

Social networking

The use of social networking sites for business and personal use is increasing. Access to social networking sites is blocked on the school systems, however a school can manage access by un-filtering specific sites, internet usage is still monitored.

School staff may need to request access to social networking sites for a number of reasons including:

- Advertising the school or managing an ‘official’ school presence,
- For monitoring and viewing activities on other sites
- For communication with specific groups of adult users eg a parent group.

Social networking applications include but are not limited to:

- Blogs
- Any online discussion forums, including professional forums
- Collaborative spaces such as Wikipedia
- Media sharing services e.g YouTube, Flickr
- ‘Microblogging’ applications e.g Twitter

When using school approved social networking sites the following statements apply:-

- School equipment should not be used for any personal social networking use
- Staff must not accept friendships from students. The legal age for students to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older.
- It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their @ <Summerhill>. dudley.sch.uk email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school
- Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.

- Postings should not be critical or abusive towards the school, staff, students or parents or used to place a student or vulnerable adult at risk of harm
- The social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way
- Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them
- It should not breach the schools Information Security policy

Data protection

The processing of personal data is governed by the Data Protection Act 1998. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the school, and not the Local Authority, to ensure that compliance is achieved.
As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the school. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the school*'s* premises or working remotely you must:-

- keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt ask your Headteacher or line manager;
- familiarise yourself with the provisions of the Data Protection Act 1998 and comply with its provisions;
- familiarise yourself with all appropriate school policies and procedures;
- not make personal or other inappropriate remarks about staff, students, parents or colleagues on manual files or computer records. The individuals have the right to see all information the school holds on them subject to any exemptions that may apply.

If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

Summerhill School

Guest User- Acceptable Use policy
Rules for Responsible Computer and Internet use

This policy applies to all community users of the schools systems, who have guest access to the internet. We trust you to use the ICT facilities sensibly, professionally, lawfully, and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please ask. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the school office.

Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying our school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply:-

- Do not download any image, text or material which is copyright protected without the appropriate authorisation.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a member of staff
- If you want to download any software, first seek permission from the member of staff responsible. They should check that the source is safe and appropriately licensed.
- You should not :
  - introduce packet-sniffing software (ie software which is used to intercept data on a network) or password detecting software;
  - seek to gain access to restricted areas of the network;
  - knowingly seek to access data which you are not authorised to view;
  - introduce any form of computer viruses;

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

Appendix 4

School Filtering Policy

School internet activity is monitored overall by Smoothwall, which is provided by the managed service but maintained, at school level, by our onsite technicians.

Smoothwall logs the internet activity of individual users and records filtered incidents. Domains and specific web addresses may be blocked to ensure the safety of students and staff and to support the acceptable use policy.

Students and staff report unsuitable sites to the Technical Resources Department who will inform the Assistant Headteacher (New Technologies) and also arrange for the blocking of the site or domain.

The school does not allow student access to Facebook, You Tube or Twitter. Staff access to You Tube is permitted.

Internet and network activities are monitored by the Assistant Headteacher (New Technologies) using Securus NG. This software records screenshots when alerted by key words or images. The categories monitored are pornography, grooming, hacking, drugs, weapons, swearing, bullying and SMS terms.

Students found to be abusing the systems are referred to the Assistant Headteacher (Pastoral) and Head of Year. The outcome of these investigations will lead to appropriate sanctions being taken. This will depend upon the seriousness of the misuse and if it is a repeated incident.

Staff misuse is reported directly to the Headteacher for appropriate action.

All staff and students are aware of the monitoring of the computer systems.

Appendix 5

Personal and Family Use of School Laptops/Personal Devices

School Laptops and Personal Devices are provided for educational purposes, such as teaching and learning, assessment, monitoring and intervention. They should not routinely be used for personal use by staff or their families.

Passwords should on no account be shared with family members and when used outside the school environment care must be taken to ensure the security of any personal data being viewed or entered. When leaving the device unattended it should be locked or shut down.

Personal data must **never** be saved on unencrypted devices or drives. You should be aware that legislation exists which may lead to a severe financial penalty for an institution or individual (Up to £500,000). CC4 Anywhere and FROG both provide secure encrypted links for accessing personal data away from school. It should be unusual and rare for personal data to be moved to an encrypted device or drive.

One drive should be used for storing electronic resources but memory sticks if used should regularly be checked to avoid introducing computer viruses to school systems.

Appendix 5

Summerhill Portable ICT Equipment
Staff Guardianship Loan Form

Name ………………………….. has permission to loan and is guardian of the following item(s) of ICT equipment (including Ipads):-

Item	**Serial No**	**Start date**	**Return date**

Whilst the above items are in your care, the school will expect you to take full personal responsibility for the safe custody of all of the items listed and to follow the guidelines below:-

- I will ensure the mobile device is secured or locked away when not in use;
- I will ensure that unauthorised software is not loaded or run on this mobile device;
- I will not download, store or collect any inappropriate material on the device
- I will ensure that all external media sources (disks, USB flash drives / memory sticks) are checked for viruses before data transfer to the mobile device where appropriate;
- I will ensure the device is regularly virus-checked where appropriate;
- I will ensure that data remains confidential and secure;
- Any personal data stored on the device will be encrypted if appropriate and removed as soon as reasonably possible
- I will ensure that the equipment is not used by anyone who has not been authorised by the school
- I will return the device upon request and when I am on leave or other absence, unless otherwise authorised.
- I will ensure the equipment is not left unattended in any vehicle (as this is not covered by the school's insurance policy), and accept that any loss arising from a loss from a vehicle will be my own responsibility.
- If the equipment is lost or stolen, I will inform the police as soon as possible to get a crime number and also contact the appropriate member of staff

Signed ………………………………… Date …/…/…

Name of person authorising the loan …………………………………..

Signed …………………………………. Date …/…/…

APPENDIX 6

Use of Computer Networks and Internet
Extract from the Behaviour Policy

It is not acceptable to:	**The consequences may be:**
Visit unsuitable websites. (Websites are filtered and monitored. Any unsuitable website that is accidentally found must be reported immediately to your teacher or the Technical Resources staff.)	Your use of the Internet can be restricted to a small number of safe domains only. Your use of computers and Internet can be monitored weekly for a fixed period.
Use school computing resources for direct chat or playing games.	Level 3 – detention
Use email during lessons unless permission has been given by your teacher as part of your learning.	Level 3 – detention
Use inappropriate language or images in documents, presentations, spreadsheets, databases, emails or any other digital media.	This is 'bullying' behaviour and will be treated in exactly the same way as verbal threats and abuse. This may involve detention, isolation, parental contact or exclusion depending on the individual circumstances.
Use email in an offensive or threatening way.	
Give out your home address in any email or at any Internet location. This can allow you to become a victim of identity theft or threaten your personal safety. **Be e-safety aware.**	
Share your password with another student. This compromises the security of your personal learning space and may allow others to misuse school systems using your identity. Always use **strong passwords** to protect your space.	
Print multiple copies of the same document or print documents unnecessarily. Printing documents unnecessarily is a waste of school resources and also is environmentally unfriendly.	Your printer credits may be reduced or withdrawn.
Play sounds or music other that when permission has been given by your teacher.	Level 3 – detention
Use passwords or hacking techniques to gain access to unauthorised files or cause malicious damage or deletion of files.	**This is a criminal offence.** This can result in a police investigation and prosecution. The school will not hesitate to prosecute offenders when necessary.