PLYMOUTH HIGH SCHOOL FOR GIRLS

POLICY: **On-line Safety Policy**

SLT LINK MEMBER:	**Pete Neve**
GOVERNORS SUB COMMITTEE:	**T & L**
This policy was adopted/updated:	**Updated April 2016**
This policy will be reviewed:	**April 2017**
Statutory Policy:	YES
Source:	South West Grid for Learning

Plymouth High School for Girls

On-line Safety Policy

Development / Monitoring / Review of this Policy

This on-line safety policy has been developed by the executive e-safety committee in consultation with:

- *Headteacher*
- *E-Safety Officer*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*
- *Parents and Carers*
- *Students*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Rationale

This policy has been developed in accordance with the principles established by the following Legislation and Guidance:

Legislation
Children Act 1989
Children Act 2004
Safeguarding vulnerable groups Act 2006
Protection of Freedoms Act 2012
Children and Families Act 2014
Education Act 2002
Adoption and Childrens Act 2002
Female Genital Mutilation Act 2003
Sexual Offences Act 2003
Children and Adoption Act 2006
Children and Young Persons Act 2008
Border, Citizenship and Immigration Act 2009
Apprenticeship, Skills Children and Learning Act 2009
Education Act 2011

Policy and Guidance
Working Together to safeguard children 2015
Keeping Children Safe in education 2015
Plymouth Safeguarding Children Board – Policies and Guidance:
http://www.plymouth.gov.uk/localsafeguardingchildrenboard/

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body on:*	March 2016
The implementation of this e-safety policy will be monitored by the:	Executive e-safety group
Monitoring will take place at regular intervals:	At least once a year
The *Governing Body* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	At least once a year as part of the annual safeguarding audit.

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	September 2017
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Simon White LA Safeguarding Co-ordinator, Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students / pupils
  - parents / carers
  - staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head-teachers to such extent as is reasonable, to regulate the behaviour of students 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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

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

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 Governors T&L Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator / Officer
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- **The *Headteacher* has a duty of care for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the *E-Safety Officer*.
- **The Headteacher and (at least) another member of the Senior Leadership Team 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.** (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR* disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders 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 Senior Leadership Team will receive regular monitoring reports from the E-Safety Officer.

E-Safety Officer:

- leads the e-safety executive committee
- takes day to day responsibility for e-safety issues (including online Prevent strategies) and has a leading role in establishing and reviewing the school 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
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments)
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The *Network Manager* is responsible for ensuring:

- **that the school's technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets required e-safety technical requirements and any Local Authority E-Safety Policy / Guidance that may apply**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep 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
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the e-safety Officer for investigation / action / sanction

- that monitoring software / systems are implemented and updated as agreed in school / academy policies

Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters (including Prevent policy) and of the current *school* e-safety policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy (AUP)**
- **they report any suspected misuse or problem to the *E-Safety Officer* for investigation / action / sanction**
- **all digital communications with students / parents / carers should be on a professional level**
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Child Protection / Safeguarding Designated Person / Officer

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

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

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives .The group will be responsible for regular reporting to the E-safety executive group who in turn report to the Governing Body.

Members of the E-safety Group (or other relevant group) will assist the E-Safety Officer with:

- the production / review / monitoring of the school e-safety policy / documents
- the production / review / monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and students about the e-safety provision

- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Students / pupils:

- **are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy**
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- 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 their membership of the school

Parents / Carers

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

- digital and video images taken at school events
- access to parents' sections of the website / VLE and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website / VLE as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems

Policy Statements

Education – students

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

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

- **A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited**
- **Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral 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. This includes the context of political and social views; British Values; Radicalisation and the threat of extremism.**

- **Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- *Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school*
- *Staff should act as good role models in their use of digital technologies, the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- *Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need*

Education – parents / carers

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

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

- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school may provide opportunities for local community groups and members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide e-safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Child-minders, youth / sports / voluntary groups to enhance their e-safety provision

Education & Training – Staff / Volunteers

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

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

- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days
- The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

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

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school / academy technical systems and devices**
- **All users will be provided with a username and secure password. Users are responsible for the security of their username and password** and will be required to change their password every 12 weeks
- **The "master / administrator" passwords for the school / academy ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place (e.g. school safe)**
- **The Business Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations**.
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school has provided differentiated filtering for staff by the use of proxy-by-pass.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Any potential or actual breach of security or technical incident should be reported to the network manager and/or business manager immediately
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems

- Staff and their families should not use school devices for personal use even when those devices are out of school
- Staff should not download executable files and/or install programmes on school devices without the agreement of the Network Manager
- An agreed policy is in place (regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

Bring Your Own Device (BYOD)

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

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

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes

- Care should be taken when taking digital / video images that students are appropriately dressed and 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 will 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 will be obtained before photographs of students are published on the school website
- Student's work can only be published with the permission of the student and parents or carers.

Data Protection

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

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

The school must ensure that:

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".**
- **It has a Data Protection Policy**
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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 using encryption and secure password protected devices.**

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

- the data must be encrypted and password protected
- the 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 (below) once it has been transferred or its use is complete
- Data stored on a 'cloud' based system such as Google must be held in such a way as to conform to the Data Protection Act (1998) and comply with the guidelines in the document 'Cloud (educational apps) software services and the data protection act (DfE October 2014).
- **At PHSG we use 'gmail' as our e-mail system and 'Google Classroom' to set and receive classwork - both of these are cloud based systems which comply with these guidelines.**
- Agreements with Cloud service providers must ensure that the provider cannot use the data for advertising or marketing purposes, as described in the DfE guidance.

Communications

✓A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓				✓			
Use of mobile phones in lessons		✓	✓				✓	
Use of mobile phones in social time	✓				✓			
Taking photos on mobile phones / cameras		✓					✓	
Use of other mobile devices e.g. tablets, gaming devices	✓						✓	
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails				✓				✓
Use of messaging apps		✓					✓	
Use of social media		✓					✓	
Use of blogs		✓					✓	

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. Users should be aware that email communications are monitored.**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication**
- **Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content**
- Students / pupils should be taught about e-safety issues such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Social Media - Protecting Professional Identity

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

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

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

School staff should ensure that:

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

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies. SWGfL BOOST includes SWGfL Alerts that highlight any reference to the school/academy in any online media (newspaper or social media) for example http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Alerts

Unsuitable / inappropriate activities

The school 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 school equipment or systems. The school policy restricts usage as follows:

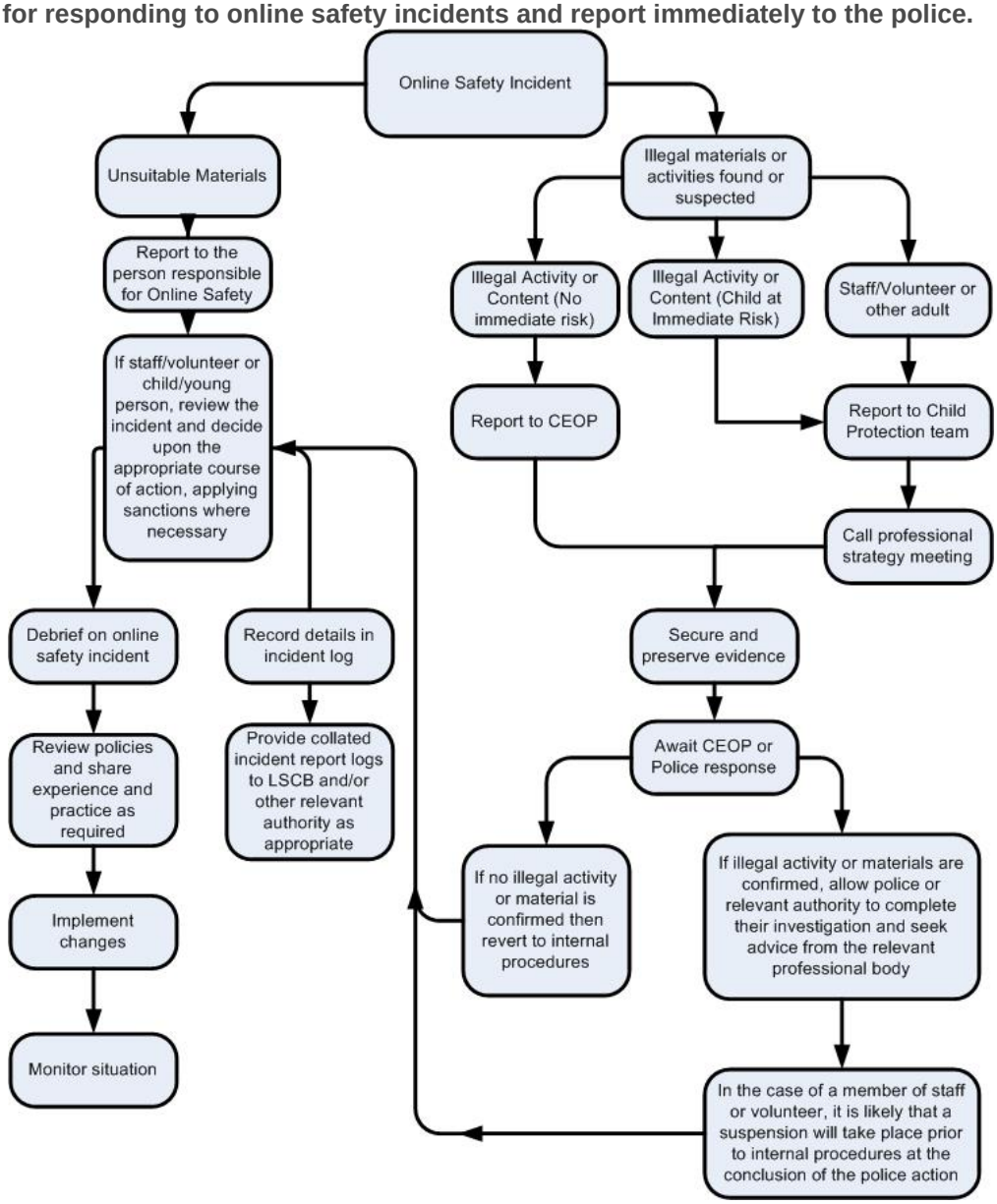
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright						X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files						X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			✓			
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce					X	
File sharing			✓			
Use of social media				✓		
Use of messaging apps			✓			
Use of video broadcasting eg Youtube		✓				

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above). SWGfL BOOST includes a comprehensive and interactive 'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool)

Illegal Incidents

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



Other Incidents

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

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

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

It is important that all of the above steps are taken as they will provide an evidence trail for the *school / academy* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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

Students / Pupils

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher /	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
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 mobile device	✓	✓				✓	✓	✓	✓
Unauthorised use of social media / messaging apps / personal email	✓	✓				✓	✓	✓	✓
Unauthorised downloading or uploading of files		✓			✓	✓	✓		✓
Allowing others to access school / academy network by sharing username and passwords		✓			✓	✓	✓		✓
Attempting to access or accessing the school / academy network, using another student's / pupil's account		✓			✓	✓	✓		✓
Attempting to access or accessing the school / academy network, using the account of a member of staff		✓			✓	✓	✓		✓
Corrupting or destroying the data of other users		✓			✓	✓	✓		✓
Sending an email, text or 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 school into disrepute or breach the integrity of the ethos of the school		✓				✓	✓		✓
Using proxy sites or other means to subvert the school's / academy'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 Actions / Sanctions

Incidents:	Refer to line manager	Refer to Head-teacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓			✓	✓
Inappropriate personal use of the internet / social media / 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 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 school / academy into disrepute or breach the integrity of the ethos of the school / academy	✓	✓				✓		✓
Using proxy sites or other means to subvert the school's / academy'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	✓	✓	✓				✓	✓

PLYMOUTH HIGH SHOOL FOR GIRLS
Student Acceptable Use Policy Agreement

School policy:

New technologies have become integral to the lives of young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

Acceptable Use Policy is intended to ensure:

Students will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. The school will try to ensure that students have good access to ICT to enhance their learning and will in return, expect the students to agree to be responsible users.

The school will ensure that any data stored on 'cloud based' systems outside of the school complies to the data Protection act and the guidance in the document 'Cloud (educational apps) software services and the data protection act (DfE October 2014).

At PHSG we use 'gmail' as our e-mail system and 'Google Classroom' to set and receive classwork - both of these are cloud based systems which comply with these guidelines.

Acceptable Use Policy Agreement:

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

I understand that the school will monitor my use of the ICT systems, email and other digital communications.

I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.

I will be aware of danger presented by people that I do not know when I am communicating online.

I will not disclose or share personal information about myself or others when on-line.

If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.

I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

I appreciate that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.

I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so. I will act as I expect others to act toward me:

I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school /

I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
I will immediately report any damage or fault involving equipment or software, however this may have happened.
I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
I will only use chat and social networking sites with permission and at the times that are allowed

When using the internet for research or recreation I recognise that:

I should ensure that I have permission to use the original work of others in my own work and that it is acknowledged and referenced appropriately.
Where work is protected by copyright, I will not try to download copies (including music and videos)
When I am using the internet to find information, I should take care to check the information I access is accurate I understand that the work of others may not be truthful and may be a deliberate attempt to mislead.

I understand that I am responsible for my actions both in and out of school and:

I appreciate the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement and when I am out of school where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, exclusions, contact with parents and, in the event of illegal activities, involvement of the police

Student Acceptable Use Agreement Form:

This form relates to the Student Acceptable Use Policy (AUP), to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the agreement access to the school ICT network will only be granted on receipt of this signed user agreement. I will use my own equipment out of school in a way that is related to me being a member of the school network when communicating with other members of the school, accessing school email, VLE, website etc.

Name Of Student

Tutor Group

Signed

Date

PLYMOUTH HIGH SCHOOL FOR GIRLS
Parent / Carer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

That parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form:

As the parent / carer of the student named below, I give permission for my daughter / son to have access to the internet and to ICT systems at school.

I know that my daughter / son has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the school internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet whilst using mobile technologies.

The school will ensure that any data stored on 'cloud based' systems outside of the school complies to the data Protection act and the guidance in the document 'Cloud (educational apps) software services and the data protection act (DfE October 2014).
At PHSG we use 'gmail' as our e-mail system and 'Google Classroom' to set and receive classwork - both of these are cloud based systems which comply with these guidelines.

I understand that my son's / daughter's activity on the school ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Student Name	
Parent / Carers Name	
Signed	
Date	

Use of Digital / Video Images:

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school.
Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media, these images may be used in presentations in subsequent lessons.
We will ensure when images are published that the student cannot be identified by the publication of their names.
Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children as stated above.

Permission Form:

As the parent / carer of the student / pupil, I agree to the school taking and using digital / video images. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, school events which include images of children other than my own, I will abide by these guidelines in my use of these images.

Student Name	
Parent / Carers Name	
Signed	
Date	

Staff and Visitor Acceptable Use Policy Agreement

School Policy:

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

Staff and visitors will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Staff are protected from potential risk in their use of ICT in their everyday work. The school will try to ensure that staff and visitors will have good access to ICT to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and visitors to agree to be responsible users.

The school will ensure that any data stored on 'cloud based' systems outside of the school complies to the data Protection act and the guidance in the document 'Cloud (educational apps) software services and the data protection act (DfE October 2014).

At PHSG we use 'gmail' as our e-mail system and 'Google Classroom' to set and receive classwork - both of these are cloud based systems which comply with these guidelines.

Acceptable Use Policy Agreement:

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

I understand that the school will monitor my use of the ICT systems, email and other digital communications.

I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school.

I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school

I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

I will immediately report any illegal, inappropriate or harmful material or incident, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems and:

Will not access, copy, remove or otherwise alter any other user's files, without their express permission.

Will communicate with others in a professional manner, not use aggressive or inappropriate language and appreciate that others may have different opinions.

Will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information those who are featured.

I will not use chat and social networking sites in school in accordance with the school's policies, will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.

I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have a responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. And will ensure that any such devices are protected by up to date anti-virus software and are free from virus.

I will not use personal email addresses on the school ICT systems

I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

I will ensure that my data is regularly backed up in accordance with relevant school policies.

I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate material which may cause harm or distress to others. I will not use any software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

I will not install (or attempt to) programmes of any type on a machine or store programs on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

I will not disable or cause any damage to school equipment or the equipment belonging to others.
I will only transport, hold, disclose or share personal information about myself or other as outlined in the School / LA Personal Data Policy (or other relevant school policy). Where personal data is transferred outside the secure school network, it must be encrypted.

I understand that Data Protection Policy requires that any staff or student data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

I will immediately report any damage or fault involving equipment or software however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

I will ensure that I have permission to use the original work of others in my own work.
Where work is protected by copyright I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school and:

I appreciate this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school but also to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

I understand that if I fail to comply with this Acceptable Use Policy Agreement I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and, in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) in accordance with these guidelines.

Staff / Visitor Name	
Signed	
Date	