The Shropshire Gateway Educational Trust

E-safety Policy

Lead Officer	Darren Reynolds, Executive Head
Approved by Board of Governors	07.11.21
Review Cycle	Annual
Next Review Date	September 2022

Development / Monitoring / Review of this Policy

This e-safety policy has been developed in conjunction with Telford and Wrekin IT services as the supplier of IT managed service for use by:

- Headteacher, Senior leaders
- E-Safety Officer / IT Lead (in many of our schools this will be the same person)
- Staff – including Teachers, Support Staff, Technical staff
- Governors and Directors
- Parents and Carers
- Community users

It will be shared with the whole school community.

Schedule for Development / Monitoring / Review

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:	1st September 2022
Should serious e-safety incidents take place, the appropriate school leads will be informed:	Executive Head teacher, Headteachers, Trust Business manager, Deputy Headteachers, IT lead, Safeguarding lead, Network Manager/Technicians

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

Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors. Breaches of this policy may be dealt with under our disciplinary policy, behaviour policy, staff discipline policy, safeguarding policy, staff code of conduct.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Trust 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 Trust, but is linked to membership of the Trust. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see DFE guidance: Searching, Screening and Confiscation). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

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

Governors / Board of Directors:

Governors/Directors 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 receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety through the Safeguarding Governor Role. The role of the E-Safety Governor / Director will include:

- receiving updates from the E-Safety/IT Lead/Technician (as required)
- receiving reports from monitoring of e-safety incident logs
- reporting to relevant Governors committee

Headteachers 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 Co-ordinator / IT Lead/ safeguarding Lead.
- **The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management 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 other relevant body disciplinary procedures).
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / IT Lead 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 / 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 / Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator / IT Lead.

E-Safety Coordinator / IT Lead:

- takes day to day responsibility for e-safety issues 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, (Examples of suitable log sheets may be found later in this document).
- meets regularly with E-Safety Governor / Director to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors / Directors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The Trust has a managed ICT service provided by an outside contractor, it is the responsibility of the Trust to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the Trust e-safety policy and procedures.

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:

- **that the school's / academy's technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the Trust meets required e-safety technical requirements and any other relevant body 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**
- filtering 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 Headteacher / Senior Leader; E-Safety Coordinator / Safeguarding Lead for investigation, action, sanction
- that monitoring software / systems are implemented and updated as agreed in Trust policies

Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters and of the current Trust e-safety policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the Headteacher / Senior Leader ; E-Safety Coordinator, IT Lead / safeguarding lead for investigation, action, sanction**
- **all digital communications with pupils / parents / carers should be on a professional level** and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies

- pupils 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 pupils 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

This person 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

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.)

Pupils:

- **are responsible for using the Trust digital technology systems in accordance with the Pupil 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 / academy'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 Trust 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 Trust 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 pupil records
- their children's personal devices in the Trust (where this is allowed)

Community Users

Community Users who access school systems / website / VLE as part of the wider Trust provision will be expected to sign a Community User AUA before being provided with access to school systems. (A Community Users Acceptable Use Agreement Template can be found in the appendices.)

Policy Statements

Education - pupils

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

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be 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**
- **Pupils 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.**
- **Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- Pupils should be helped to understand the need for the pupil 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 pupils 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 pupils 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.

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

- Curriculum activities
- 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

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.** It is expected that some staff will identify e-safety as a training need within the performance management process.
- **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 / IT Lead (or other nominated person) will receive regular updates through attendance at external training events, 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 as appropriate.
- The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors / Directors

Governors / Directors 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 Trust / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The Trust has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the Trust E-Safety Policy / Acceptable Use Agreements.

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:

- **Trust technical systems will be managed in ways that ensure that the Trust meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school academy technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to Trust technical systems and devices.**
- **All users will be provided with a username and secure password** by the IT Lead who will keep an up to date record of users and their usernames. **Users are responsible for the security of their username and password** and will be required to change their password periodically). (Schools / Academies may choose to use group or class log-ons and passwords for KS1 and below, but need to be aware of the associated risks – see appendix)
- **The "master / administrator" passwords for the Trust 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 IT Lead **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** (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- **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 enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)
- Trust 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
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Temporary access of "guests" can be facilitated (e.g. trainee teachers, supply teachers, visitors) onto the school systems but these guests must comply with the contents of this policy.
- Personal data (as defined in GDPR) 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
- Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Use of digital and video images

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

- **When using digital images, staff should inform and educate pupils 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 in 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 pupils 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' 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 pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil 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 Trust 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)**
- 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

Please refer to the Trust Data Protection Policy for more information

Communications

This is an area of rapidly developing technologies and uses. This section may also be influenced by the age of the pupils. The table has completed considering this for Secondary and Primary schools. (S – Secondary School in trust: P – Primary Schools in trust). 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				Pupils			
Communication Technologies	Not Allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones may be brought to school		S	P		P			
Use of mobile phones in lessons	SP				P			S
Use of mobile phones in social time			PS		P		S	
Taking photos on mobile phones / cameras			S	P	P		S	
Use of other mobile devices e.g. tablets, gaming devices	SP				P			
Use of personal email addresses in school, or on school network	SP				SP			
Use of school email for personal emails	SP				SP			

Use of messaging apps			PS		P		S	
Use of social media				PS	P		S	
Use of blogs		PS						P

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

- **The official Trust /school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** Staff and pupils should therefore use only the Trust email service to communicate with others when in school, or on Trust systems (e.g. by remote access).
- **Users must immediately report, to the nominated person – in accordance with the Trust 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 pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.** These communications may only take place on official (monitored) Trust systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual Trust email addresses for educational use.
- 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 Trust website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the Trust 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.
- 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 pupils, parents / carers or school staff

- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school /academy 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

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from Trust and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. 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.

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 Trust					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. 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	

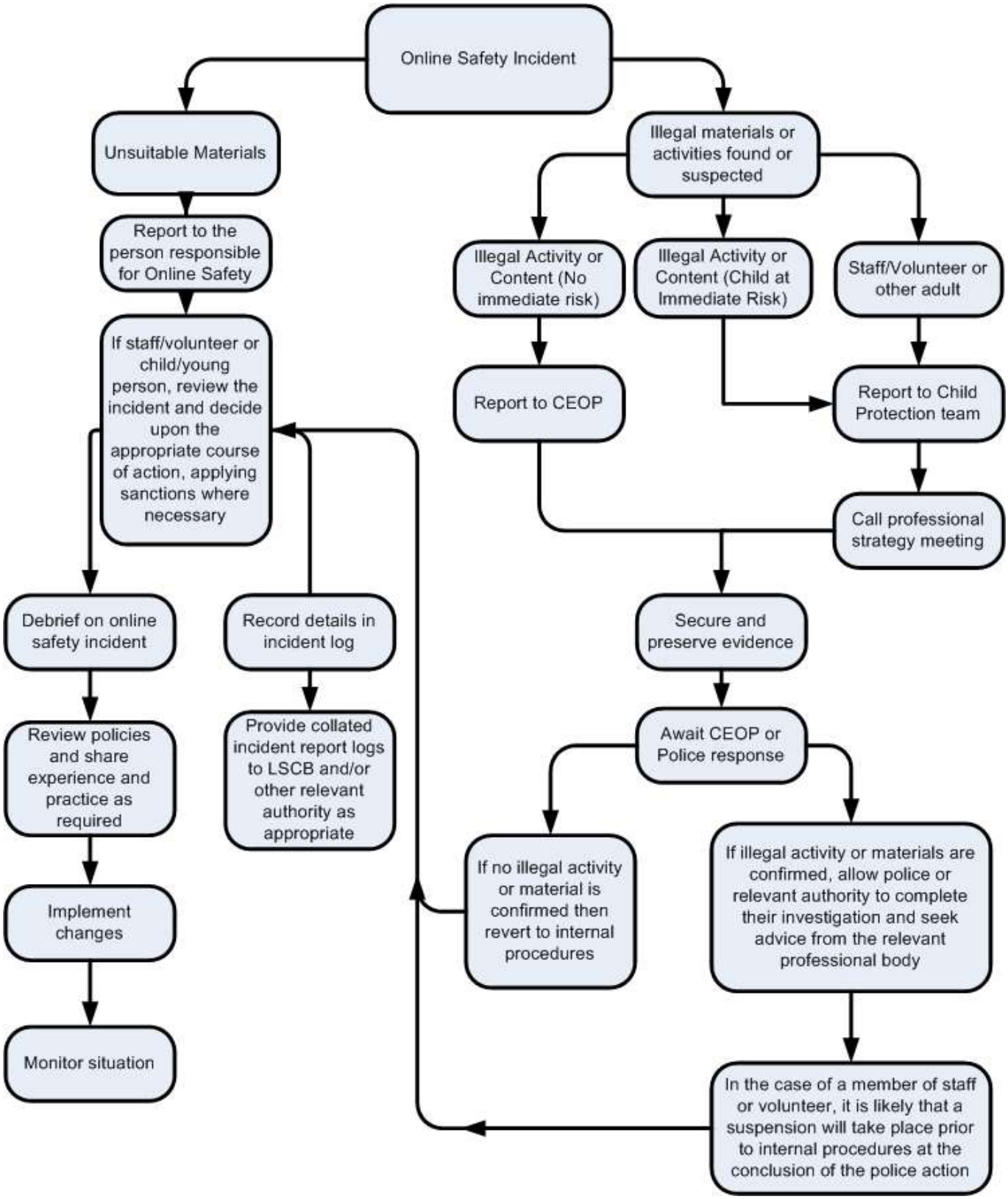
On-line gaming (educational)				X	
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce				X	
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. YouTube			X		

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).

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.


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

Other Incidents

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

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of Child 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 Trust 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.

Trust Actions & Sanctions

It is more likely that the Trust 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:

Pupils

Actions / Sanctions

(* indicates use if repeated incident)

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

Staff

Actions / Sanctions

(* indicates use if repeated incident)

Incidents:	Refer to line manager	Refer to Headteacher Principal	Refer to Directors	Refer to Police (and following children protection policy)	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).		X	X	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email		x				x		X*
Unauthorised downloading or uploading of files		x			x	x		X*
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		x			x	x		X*
Careless use of personal data e.g. holding or transferring data in an insecure manner		x				x		X*
Deliberate actions to breach data protection or network security rules		x	x				x	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x				x	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x				x		X*
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		x		(X)	x	x	x	x
Actions which could compromise the staff member's professional standing		x				x		X*
Actions which could bring the Trust into disrepute or breach the integrity of the ethos of the Trust		x				x		X*
Using proxy sites or other means to subvert the school's / academy's filtering system		x			x		x	X*
Accidentally accessing offensive or pornographic material and failing to report the incident		x				x		
Deliberately accessing or trying to access offensive or pornographic material		x		x				x
Breaching copyright or licensing regulations		x				x		
Continued infringements of the above, following previous warnings or sanctions		x	x					x

Incident Log sheet

Please complete this log for all e-safety incidents. **Please note this does not replace referring incidents as appropriate to the LADO, police or children's services as per the e-safety incident flow chart.**

Appendix H: *E-Safety Incident Reporting Log*						
Date	*Time*	*Incident*	*Action Taken*		*Incident Reported By*	*Signature*
			What?	*By Whom?*		

Appendix A - AUP for Staff, Governors & Volunteers

I understand that I have personal and legal responsibilities, including treating others with dignity and respect, acting honestly, using public funds and school equipment appropriately, adhering to health and safety guidelines and safeguarding pupils at all times.

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

I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to benefit from the use and application of appropriate digital technology.

I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with children and young people.

Professional and personal safety:

- I understand that the school has in place a filtering system and will monitor my access to digital technology and communications systems whilst using school devices, and/or access to the school network via personal devices, where such access has been granted.
- I understand that the rules set out in this agreement also apply to use of school devices and digital technologies out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use in line with the e-safety policy and the expectations of professional behaviour set out in the Staff Code of Conduct.
- 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 understand that I should keep passwords safe and not share them with anyone.
- I will immediately report any incidence of access to illegal, inappropriate or harmful material, deliberate or accidental, by myself or others, to the appropriate person.
- I will not install or attempt to install programmes of any type on a device, nor will I try to alter computer settings, unless this is permitted by the Network Manager.
- I will not deliberately 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 others, as outlined in the Data Protection Policy
- 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 required by law, or by school policy, to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving devices or software, however this may have happened.
- 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 will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will log out of a device when I have finished using it.

Electronic communications and use of social media:

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will use social networking sites responsibly, taking care to ensure that appropriate privacy settings are in place, and ensure that neither my personal nor professional reputation, nor the school's reputation, is compromised by inappropriate postings, to include past postings.
- I will never send or accept a 'friend request' made through social media from a student at school. I understand that such requests should be raised formally as an incident.
- I will not, under any circumstances, make reference to any staff member, student, parent or school activity/event via personal social media or other communication technologies.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner. At no time will I use or share a personal email address, phone number or social networking site for such communication purposes.
- I will notify the Headteacher of any current or future, direct or incidental contact with students, parents or carers, for example where parents or carers are part of the same social group
- I will not engage in any online activity, at, or outside school, that may compromise my professional responsibilities. This includes making offensive, aggressive or defamatory comments, disclosing confidential or business-sensitive information, or information or images that could compromise the security of the school.
- I will not use the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material, online or in print.
- I will not post any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school.

Use of school and personal mobile devices and technologies

- When I use my own mobile device (e.g. laptop / tablet / mobile phone / USB device) 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. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
    - I will keep my personal phone numbers private and not use my own mobile phone, or other device, to contact students or parents in a professional capacity.
    - I will keep my mobile phone secure whilst on school premises. It will be switched off whilst I am on duty unless there are good reasons that have been approved with a member of the senior leadership team, and then that is discreet and appropriate, e.g. not in the presence of students.
    - I will keep mobile devices switched off and left in a safe place during lesson times. I understand that the school cannot take responsibility for personal items that are lost or stolen.

- I will report any text or images sent to me by colleagues or students which could be viewed as inappropriate. I will not use a personal device to photograph a student(s), except with the written permission of the Headteacher.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails if I have any concerns about the validity of the email or its source is neither known nor trusted.
- I will, when I take and/or publish images of others, do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use any personal devices to record these images, unless I have written permission from the Headteacher. Where these images are approved by the school to be published (e.g. on the school website) it will not be possible to identify by name, or any other personal information, those who are featured.
- I will not attempt to upload, download or access any material which is illegal (for example; images of child sexual abuse, criminally racist material, adult pornography), inappropriate or may cause harm or distress to others. I will not attempt 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 not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

Conduct and actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school devices and digital technology in school, but also applies to my use of school systems and equipment off the premises. This Acceptable Use Policy also applies to my use of personal devices on the premises or in situations related to my employment by the school.
- I understand that should I fail to comply with this Acceptable Use Policy Agreement, I may be subject to disciplinary action in line with the school's agreed Disciplinary Procedure. In the event of any indication of illegal activity, I understand the matter may be referred to the appropriate agencies.

I have read and understood the above, and agree to use school devices and access digital technology systems (both in and out of school), as well as my own devices (in school and when carrying out communications related to the school), within this agreement.

I understand that in the event of any query or concern about this Agreement, I should contact the Headteacher.

Staff / Volunteer Name:	
Signed:	
Date:	

Appendix B - AUP for learners in KS1

I want to feel safe all the time.

I know that anything I do on the computer can be seen by other people.

I know when to use the CEOP report button

I agree that I will:

- not use my own mobile phone, or any other device, in school, unless I am given permission
- always keep my passwords safe and not share them with anyone
- only open web pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or unhappy on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel sad or worried
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home, my family or my pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Signed _____ ***Date*** _____

Appendix C - AUP for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

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

I know that anything I share online may be monitored by school.

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.

I agree that I will:

- always keep my passwords safe and not share them with anyone
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved, and I will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe, worried or uncomfortable
- not reply to any nasty message or anything which makes me feel unhappy or worried
- not use my own mobile phone, or any other device, in school, unless I am given permission
- only give my mobile phone number to friends I know and trust in real life
- only email people I know or are approved by my school
- only use email which has been provided by school
- obtain permission from a teacher before I order online
- discuss and agree my use of a social networking site with a responsible adult before creating a profile or signing up for an account
- always follow the terms and conditions when using a website
- always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me

Signed _____ ***Date*** _____

Appendix D - AUP for learners in KS3 and above

The policy aims to ensure that any communications technology is used without creating unnecessary risk to others.

I agree that I will:

- respect the school network security
- set strong passwords which I will not share
- only use, move and share personal data securely
- not use my own mobile phone, or any other device, in school, unless I am given permission
- only visit sites which are appropriate
- always follow the terms and conditions when using a website
- respect copyright and the intellectual property rights of others
- only create and share content that is legal
- discuss and agree my use of a social networking site with a responsible adult before joining
- not access social networking sites whilst at school
- obtain permission from a teacher before I order online
- only use approved email accounts
- only use appropriate content which I have permission to use
- only communicate online with trusted users
- never meet an online friend without taking a responsible adult that I know with me
- make sure all messages/posts I send are respectful
- not respond to or forward any inappropriate message or content
- be cautious when sharing personal contact information
- only communicate electronically with people I know or have been approved by my school
- report unsuitable content or activities to a member of staff

I know that anything I share online at school via the school network may be monitored by the school.

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.

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

I agree that I will not:

- act in a way that might breach the school Behaviour policy
- forward chain letters
- breach copyright law
- do anything which exposes others to harm or danger
- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - inappropriate images
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts

I accept that my use of both school and personal devices may be monitored and reported on.

Signed _____ ***Date*** _____

Appendix E– ***Sample Home-school E-safety; ICT, Mobile Phones, Personal Photographs and Social Media***

Student Name	
Student's class teacher/form name	
Parent/Carer/Guardian's name	

Use of School ICT Equipment and Internet Access

As the parent or legal guardian of the above-named student, I give permission for my child to access the Internet, school email and other ICT facilities, whilst at school. I understand that my child has signed an Acceptable Use Policy (AUP) confirming their understanding and acceptance of the proper use of school and personal ICT equipment. I also understand that my child may be informed, should the rules change or be updated, during the year.

I accept that ultimately, the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep students safe and to prevent them from accessing inappropriate materials. These steps include the school using a filtered internet service, providing secure access to email, employing appropriate teaching practice and teaching e-safety skills to students, across the curriculum.

I understand that the school can monitor my child's computer files and the Internet sites they visit. I also understand that the school may contact me if there are concerns about my child's online behaviour or safety. I will support the school by promoting safe use of the internet and digital technology at home, and will inform the school if I have any concerns about my child's e-safety.

Mobile Phones and other Personal Devices

Primary version:

I understand that if my child has a mobile phone it should be handed into the office at the beginning of the day and collected at the end of the day (primary). I understand that 'Smart' watches or similar must not be brought to school under any circumstances.

Secondary version:

I understand that unless my child is given permission by a teacher, their mobile phone and any other personal device should be switched off and kept out of sight during the school day. This includes during off-site activities. If my child breaks this rule, I understand that the phone or device will be confiscated and I will be asked to collect it in person, at the end of the school day.

Personal Photographs and Social Media

I am aware that the school permits parents/carers to take photographs and videos of their own children at school events but requests that where the photos/videos contain

images of other children, these are not shared on any social networking site such as Facebook or Instagram. I will support the school's approach to e-Safety and will not post, upload or add any text, image or video that could upset, offend or threaten the safety of any member of the school community

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident

Signature of Parent/Carer/Guardian:

Date: