E-Safety Policy

'Let us protect with love all that God has given us.'

Introduction
The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to E-Safety. The policy relates to other policy and procedures including the school Safeguarding Policy (and Government document 'Keeping Children Safe in Education'), the staff/volunteer induction process, The Acceptable Use Agreements and the ICT and PSHCE curriculum.

This E-Safety policy was approved by the Governing Body on:	
The policy will be monitored by the E-Safety Committee:	**Computer Coordinator** **Member of SLT** **(Safeguarding/Health & Safety)** **Computer Governor** **Turn it On Technician**
The Policy was written in consultation with:	• Pupils • Wider community • Parent/Carers
The E-Safety Policy will be monitored and 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 Autumn 2018.	Annually Autumn Term
Should serious E-Safety incidents take place, the following external persons / agencies should be informed:	

Scope of the Policy
This policy applies to all members of the school community (including staff, 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 Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place 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 for template policy). 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, safeguarding 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. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- meetings with the E-Safety Co-ordinator and the E-Safety group meetings
- regular monitoring of E-Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to Governors as appropriate

Headteacher:

- 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
- The Headteacher (Designated Safeguarding Lead) and Deputy Safeguarding Leads are aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff
- The Headteacher is responsible for ensuring that the E-Safety Coordinator 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 will receive regular monitoring updates from the E-Safety Co-ordinator

E-Safety Coordinator:

- Leads the E- safety group
- Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies / documents
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments
- 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 advice for staff
- Liaises with school technical staff
- Meets with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs and attends relevant meetings with Governors
- Reports regularly to the Headteacher

Technical staff (Turn it On – external provider):

Turn it On is responsible for ensuring:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets required E-Safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply
- Users may only access the networks and devices through a properly enforced password protection procedure

- Filtering is applied and updated on a regular basis and complies with the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet
- 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
- Use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- Monitoring software / systems are implemented and updated as agreed with the school

Teaching and Support Staff: are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Agreement (AUA)
- They report any suspected misuse, safeguarding issue or problem to the Headteacher for investigation, action or 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 agreements 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: is trained in E-Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- 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
- At an age appropriate level, 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 as set out in the Home School Agreement signed by parents/carers on pupil's entry to 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 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 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 as part of the wider school provision will be expected to sign an acceptable use agreement (AUA) before being provided with access to school systems.

Policy Statements - Education

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 is a focus in all areas of the curriculum and E-Safety messages are reinforced E-Safety across the curriculum. The E-Safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned E-Safety curriculum is provided as part of Computing / PSHCE / other lessons and is regularly revisited
- Key E-Safety messages are reinforced as part of a 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision making
- 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

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
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.thinkyouknow.co.uk(CEOP)

The Parent/carers are reminded that the school's E-Safety Policy covers their actions out of school as set out in the Home School Agreement signed by parents/carers on pupil's entry to the school where it states that pupils will not engage in using social media whilst at St Josephs.

Education – The Wider Community

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

- Providing open evenings, workshops and printed material on the use of new digital technologies, digital literacy and E-Safety
- E-Safety messages are targeted towards grandparents and other relatives as well as parents
- The school website will provide E-Safety information for the wider community
- Liaise with other organisations/schools as appropriate

Education & Training – Staff / Volunteers

It is essential that all staff 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.
- All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable Use Agreements
- The E-Safety Coordinator will receive regular updates through Oxfordshire updates and attending training and by reviewing guidance documents released by relevant organisations (such as Safer internet centre)
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings
- The E-Safety Coordinator 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 Curriculum and Pupils committee. 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 (this may include attendance at assemblies / lessons)

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 are outsourced and 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 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 technical systems and devices

Licences

- The School 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

Password Security

- All users will be provided with a username and secure password. Users are responsible for the security of their username and password
- The 'master' passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- Users will '*lock*' or '*log out'* of computers when leaving them unattended

Filters

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider
- Filtering content lists are regularly updated and internet use is logged and regularly monitored and members of SLT have passwords to access the systems to monitor
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet
- There is a clear process in place to deal with requests for filtering changes
- The school has provided enhanced / differentiated user-level filtering

Monitoring

- School technical staff monitor the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. Members of SLT have a password to access the systems to monitor
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed

Malicious Cyber Attacks

- 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

User Agreements

- An agreed system is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems
- The school has drawn up *'Acceptable Use Agreements'* for pupils, staff and volunteers
- An acceptable use agreement is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school
- An agreed policy is in place that allows staff to download executable files and installing programmes on school devices which are appropriate to their teaching and are being used for school purposes

Data

- 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. However, teaching staff are able to access documents from school via the VPN or through using Outlook 360 one drive

Use of Non-School Equipment including Mobile Phones

- The school Acceptable Use Agreements for staff, pupils and parent/carers will give consideration to the use of mobile technologies
- The School allows:

	School Devices			**Personal Devices**		
	School owned for single user	**School owned for multiple users**	**Authorised device***	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	No	Yes**	Yes***
Full network access	Yes	Yes	Yes	No	No	No
Internet only					Yes	By arrangement
No network access						

* Authorised device – purchased by pupil/family through a school organised scheme. This device may be given full access to the network as if it were owned by the school.

** Staff owned personal devices are allowed in school – for use in the staff room and offices. They must not be used in classrooms or playground during school hours.

*** Visitor owned devices may only be used in the staffroom and office area.

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 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 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
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press (covered as part of an agreement signed by parents or carers at the start of the academic year)
- 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; <u>the personal equipment of staff should not be used for such purposes</u>
- 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
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs, unless express parental permission has been sought beforehand
- 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 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 (ICT Disaster Recovery Play by Turn it On)
- 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 – including the VPN or Outlook One Drive when using data off site

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

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. 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. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)
- 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 pupils or parents / carers (email, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications
- 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 and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber-bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school 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:

- Ensuring personal information is not published
- 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 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 E-Safety coordinator.

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

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:

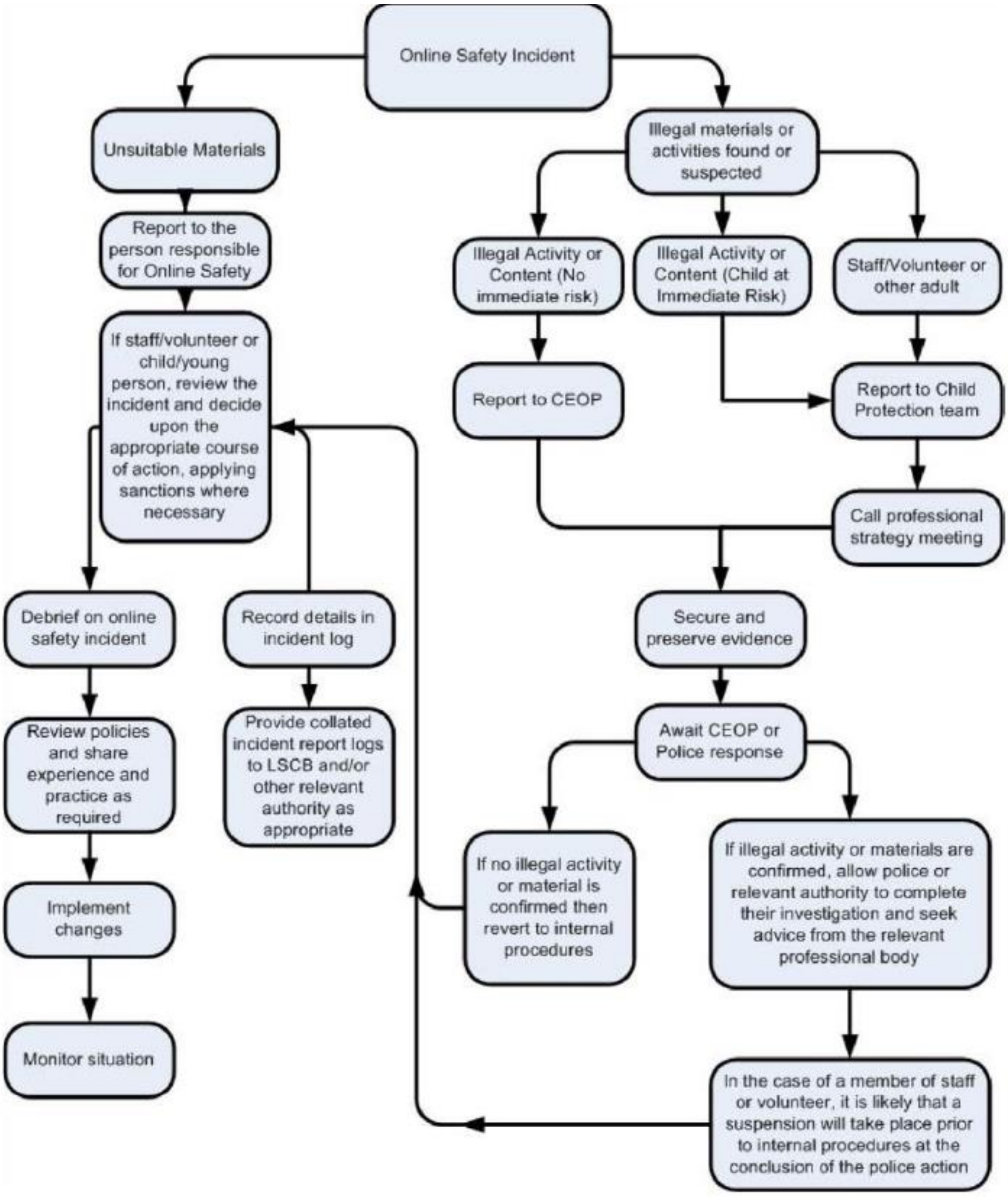
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and Illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child 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 the 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	
	Promotion of extremism or terrorism				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					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 (such as 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			X			

Responding to incidents of misuse

This guidance is intended for use when staff needs 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 school 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 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 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.

Pupil Incidents	**Refer to class teacher**	**Refer to Coordinator**	**Refer to Headteacher/DSL**	**Refer to Police/MASH**	**Refer to ICT Support for logging**	**Inform parents/carers**	**Removal of ICT/Internet access**	**Warning**	**Further sanctions**
Deliberately accessing or trying to access material that could be considered illegal			X						
Unauthorised use of non-educational sites during lessons	X								
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device			X						
Unauthorised/inappropriate use of social media/messaging apps/personal email			X						
Unauthorised downloading or uploading of files	X								
Allowing others to access the school network, by sharing username or passwords	X								
Attempting to access or accessing the school network, using another pupil's account	X								
Attempting to access or accessing the school network, using the account of a member of staff		X							
Corrupting or destroying the data of another user	X								
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X						
Continued infringements of the above following previous warnings or sanctions			X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.			X						
Using proxy sites or other means to subvert the school's academy's filtering system		X							
Accidentally accessing offensive or pornographic material and failing to report the incident	X								
Deliberately accessing or trying to access offensive or pornographic material			X						
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X							

Staff Incidents	Refer to Coordinator	Refer to Headteacher/DSL	Refer to HR	Refer to Police /LADO	Refer to ICT Support for logging	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal				X				
Inappropriate personal use of internet/social media/ personal email		X						
Unauthorised downloading or uploading of files		X						
Allowing others to access the school network, by sharing username or passwords or attempting to access or accessing the school network, using another person's account			X					
Careless use of personal data e.g. holding or transferring data in an insecure manner		X						
Deliberate actions to breach data protection or network security				X				
Corrupting or destroying the data of another user or causing deliberate damage to hardware or software			X					
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X					
Using personal email/ social networking / instant messaging/ text messaging to carry out digital communications with pupils				X				
Actions which could compromise the staff member's professional standing			X					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X						
Using proxy sites or other means to subvert the school's filtering systems		X						
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X			X
Deliberately accessing or trying to access offensive or pornographic material				X				
Breaching copyright or licensing regulations	X							
Continued infringements of the above, following previous warnings or sanctions			X					

Date Passed:

Review Date:

Signed:

Information and Communications Technology
Acceptable Use of Internet Agreement – EYFS/KS1

'Let us protect with love all that God has given us.'

ST JOSEPH

Pupil and Parent Agreement

This is how I stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer/tablet.

Pupil's signature ………………………………………………………. Date ………………………………..

Parent/Carer

As the parent or legal guardian of the pupil signing above, I give permission for my son or daughter to use the internet, under supervision, at school.

I understand and accept the above rules for acceptable use of the internet and will discuss these with my child.

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 internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet.

I will encourage my child to adopt safe use of the internet and digital media at home.

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.

I understand that allowing my child to play computer or on-line games that are not PEGI age appropriate may be considered a safeguarding issue which the school is under obligation to take action on.

I have read and understood the Parent/Carer Code of Conduct with regards to digital media.

I will not allow my child to have a social media, messaging or networking account that is not age appropriate (e.g. Facebook, WhatsApp, Instagram, Snapchat, You Tube etc.) – as set out in our home school agreement.

Parent/Carer's signature ……………………………………………. Date ………………………………..

Pupil's name ……………………………………………… Class ……………………

Information and Communications Technology
Acceptable Use of Internet Agreement – KS2

'Let us protect with love all that God has given us.'

Pupil and Parent Agreement

When I am at school , I understand I must use the school systems in a responsible way and ensure that there is no risk to my safety or the safety and security of the systems and other users. I will keep these agreements:

- I will not bring a mobile phone or other device to school including devices I can take pictures with *(Mobile phones for Year 5/6 must be handed into the office, switched off, before the start of the school day and may be collected after the bell at the end of the day)*
- I will only use the internet with permission, when there is a teacher or adult helper present
- I will keep my username and password safe and secure – I will not share it, nor will I use any other person's username and password.
- I will not try to find unsuitable sites on the internet
- I will be aware of 'stranger danger' when I am communicating on line and not give my full name or home address or telephone number, or arrange to meet someone
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on line.

Outside of school, I will keep these agreements made with my parent/carer:

- I will not have a social media, or messaging or networking account that is not age appropriate (e.g. Facebook, WhatsApp, Instagram, Snapchat, You Tube etc.) – as set out in the home school agreement.
- I will only message people I know, or whom my parents/carers have approved
- The messages I send will be polite and sensible
- I will not give my full name or home address or telephone number, or arrange to meet someone unless my parent/carer has given permission
- I will not take, use, share , publish or distribute images of other pupils without their permission and the permission of their parent/carer

Pupil's signature ……………………………………………………… Date ………………………………..

Parent/Carer

As the parent or legal guardian of the pupil signing above, I give permission for my son or daughter to use the internet, under supervision, at school.

I understand and accept the above rules for acceptable use of the internet and will discuss these with my child.

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 internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet.

I will encourage my child to adopt safe use of the internet and digital media at home.

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.

I understand that allowing my child to play computer or on-line games that are not PEGI age appropriate may be considered a safeguarding issue which the school is under obligation to take action on.

I have read and understood the Parent/Carer Code of Conduct with regards to digital media.

I will not allow my child to have a social media, messaging or networking account that is not age appropriate (e.g. Facebook, WhatsApp, Instagram, Snapchat, You Tube etc.) – as set out in our home school agreement.

Parent/Carer's signature …………………………………………… Date ………………………………..

Pupil's name ……………………………………………… Class ……………………

Information Systems Code of Conduct
Acceptable Use Agreement – Staff/Volunteers/Temporary Users

'Let us protect with love all that God has given us.'

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of 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 young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) 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 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- 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 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 full name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils 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.

Education

- I ensure that E-Safety issues are embedded in all aspects of the curriculum and other activities and pupils understand and follow the E-Safety and acceptable use policies
- I ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- I will monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current agreements with regard to these devices
- In lessons, where internet use is pre-planned, I will guide pupils to sites checked as suitable for their use
- I follow the processes that are in place for dealing with any unsuitable material that is found in internet searches

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

- When I use my mobile devices (laptops / tablets / 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. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (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 or may cause harm or distress to others. I will not 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 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 install programmes of any type on a machine, or store programmes 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 / academy 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 School / Academy / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil 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 / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- No other family member or friend will use my school devices

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 the *school / academy*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school / academy digital technology equipment in school, but also applies to my use of school / academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy
- 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 / Directors 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 digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines. I have read and understood the school E-Safety Policy.

Signed: ………………………………………… Date: ………………………………………..
Name: …………………………………………

Quick Guide to E-Safety for Staff

To ensure that staff are fully aware of their professional responsibilities when using school information systems, they are asked to sign a code of conduct. key areas include:

Roles and Responsibilities	• I have an up to date awareness of E-Safety matters and have read and understood the current E-Safety Policy • I will keep up to date with changes in E-Safety policy and practice • I will report immediately any suspected misuse, safeguarding issue or problem to the Safeguarding lead • I have read and understood what constitutes as misuse and how the school will respond
Education	• I ensure that E-Safety issues are embedded in all aspects of the curriculum and other activities and pupils understand and follow the E-Safety and acceptable use policies • I ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • I will monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current agreements with regard to these devices • In lessons, where internet use is pre-planned, I will guide pupils to sites checked as suitable for their use • I follow the processes that are in place for dealing with any unsuitable material that is found in internet searches
Technical – infrastructure / equipment, filtering and monitoring/Data	• The information systems are school property and I understand that it is a criminal offence to use a computer for purposes not permitted by the owner • I will ensure that my school information systems use will always be compatible with my professional role • I understand that the school may monitor my information systems and internet use to ensure policy compliance • I will respect system security and will not disclose any password or security information to anyone other than an appropriate systems manager • I will not install any software or hardware without permission • I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely – following the guidelines set out in the E-Safety policy • I will respect copyright and intellectual property rights • I will use appropriate channels to bypass our school filtering systems and will not bypass them without permission using the school procedure • No family or friends will use my school devices
Use of Digital and Social Media	• I will follow the policy guidance on communications, use of digital images and use of social media • I will not use personal devices to take pictures or video of pupils • I will not make reference, in social media, to pupils, parents/carers or school staff • I will not engage in online discussion on personal matters relating to members of the school community • I will not attribute my personal opinions to the school • I will check my security settings on personal social media profiles to minimise risk of loss of personal information
Communication	• I will follow the policy guidance on use of mobile phones at school and will not use my mobile phone while in school (except when I am on a break and not responsible for pupils) • All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems