Crockerne Church of England Primary School

E-safety Policy

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by the 'e-safety team': E-Safety/Computing lead, Esafety/Computing Governer, Safeguarding Governor, Designated Safeguarding Lead (DSL) IT Technician and Co-headteacher.

Schedule for Development / Monitoring / Review

This E-Safety policy was approved by the Governing Body on:	*April 2021*
The implementation of this E- Safety policy will be monitored by the:	*E-safety team*
Monitoring will take place at regular intervals:	*Annually (or more regularly if appropriate)*
The Governing Body will receive a report on the implementation of the E- Safety Policy (which will include anonymous details of esafety incidents) at regular intervals:	*Annually (or more regularly if appropriate)*
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:	*April 2022*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer: Joanne Bocko: 01275 885507* *Simon Marriott (CEO): 01934 628651* *DOFA: 01275 888211* *Police: 111*

The school will monitor the impact of the policy using: Logs of reported incidents

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

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology 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 online-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 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 online safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the E- Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Curriculum, Standards and Staffing Sub Committee (CSS) receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E- Safety Governor. The role of the E- Safety Governor will include:

- regular meetings with the E-safety/Computing lead
- attendance at E- Safety Group meetings
- regular monitoring of e- safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Committee meetings

Co-Headteachers and Senior Leaders

- The Co- Headteachers have a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the E-safety/Computing lead
- The Co-Headteachers and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents –

included in a later section – "Responding to incidents of misuse" and relevant Local Authority / MAT / other relevant body disciplinary procedures).

- The Co-Headteachers are responsible for ensuring that the E- Safety/Computing lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Co-Headteachers will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-safety/Computing lead

E- Safety/Computing Lead:

- 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 online 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 school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future online safety developments
- Meets regularly with E-safety/Computing Governor to discuss current issues, review incident logs and filtering / change control logs
- Reports regularly to Senior Leadership Team

Network Manager / Technical staff

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

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and other relevant E-safety Guidance that may apply.

- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Co- Headteachers and E-safety/Computing Lead for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school / academy policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school 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 Co-Headteachers / E- Safety Lead for investigation/ action / sanction
- all digital communications with students / 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
- students / pupils understand and follow the E-safety Policy and acceptable use policies
- students / 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 students / 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

Designated Safeguarding Lead

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
- online-bullying

E-safety Group

The E-safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the E- Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the E- Safety Group will assist the E- Safety Lead with:

- the production / review / monitoring of the school E- Safety Policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes.
- reviewing the E- safety / digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Students / Pupils:

- are responsible for using the school digital technology systems in accordance with the 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
- 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 onlinebullying.

- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E- Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website 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)

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 / digital literacy 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 broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e- safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e- safety messages should be reinforced as part of assemblies
- 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.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the 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 online 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:

- 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. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

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:

- All teaching staff will undergo annual e-safety training. Any updates will be shared as appropriate.
- All new staff should receive online 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 Lead will receive updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.

  This E-safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-safety Lead will provide advice / guidance / training to individuals as required.

Training – Governors

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

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

Technical – infrastructure / equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password.

- The “administrator” passwords for the school ICT systems, used by the Network Manager must also be available to the Co-Headteachers or other nominated senior leader and kept in a secure place
- IT Techcnician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content 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
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.

- The school has provided differentiated user-level filtering
- IT Technician monitors and records 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.
- An agreed policy is in place (a guest wi-fi log in with limited access) for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- The staff acceptable use policy defines: the extent of personal use that users are allowed on school devices that may be used out of school; guidance on downloading executable files and installing programmes on school devices and procedures regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's E- Safety education programme.

 The school Acceptable Use Agreements for staff, pupils/students and parents / 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*	*Yes- left in office*	*Yes- left in staff room*	*Yes- left in staff room/office*
Full network access	*Yes*	*Yes*	*Yes*		*Yes*	*No*
Internet only						*Yes*
No network access				*Yes*		

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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take digital images of their children at school events only when specified by the coheadteachers 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 students / 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.
- 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 current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- 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.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.

- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools (n.b. including Academies, which were previously exempt) must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

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.

Communications

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

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

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

- The official school email service may be regarded as safe and secure and is monitored. Users must immediately report, to the co-headteachers – 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, social media, chat, blogs, VLE etc) must be professional in tone and content.

- 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, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or MAT 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:

- Ensuring that personal information is not published
- Training is provided including: 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 MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures Personal

  Use:

- Personal communications are those made via a personal social media accounts. 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 upon 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
- The school permits reasonable and appropriate access to private social media sites during break times

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by E-safety Group to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school 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 or outside the 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, downloac 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	
	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	

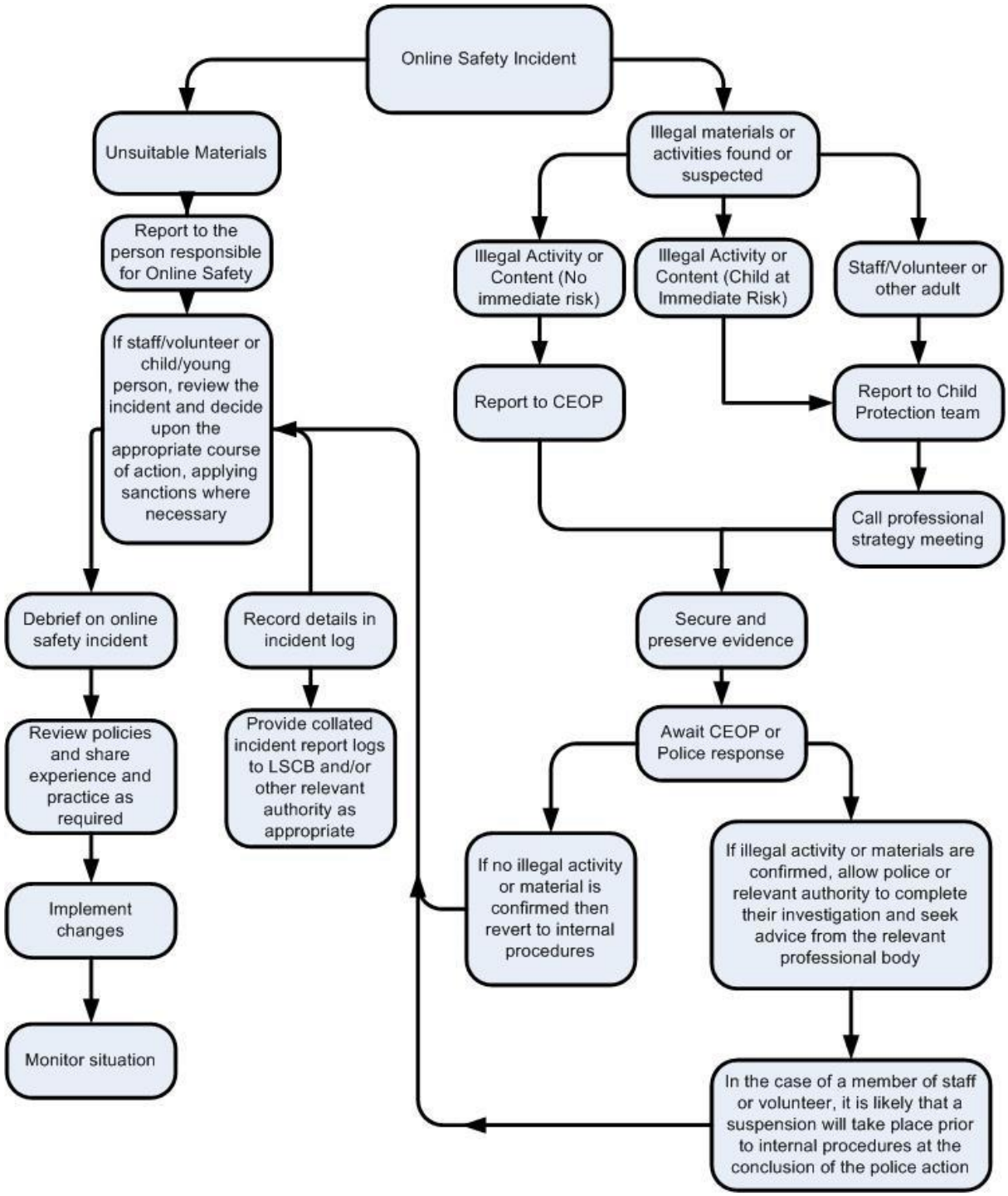
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		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.



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 / MAT
    - 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
    - promotion of terrorism or extremism
    - 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 safeguarding purposes.

The completed form should be retained by the group for evidence and reference purposes.

School / Academy 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 disciplinary procedures as follows:

	Actions / Sanctions								
Students / Pupils Incidents	Refer to class teacher	Refer to Senior Leader	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / securityetc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	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 school network by sharing username and passwords			X						
Attempting to access or accessing the school network, using another student's / 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 other users	X								
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X		X			X			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			X			
Deliberately accessing or trying to access offensive or pornographic material	X		X		X	X			

Actions / Sanctions

Staff Incidents	Refer to line managerr	Refer to Headteacher	Refer to Local Authority /MAT	Refer to Police	Refer to Technical Support Staffl 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				
Inappropriate personal use of the internet / social media / personal email		X						
Unauthorised downloading or uploading of files		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						

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 rules		X						
Corrupting or destroying the data of other users 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 carrying out digital communications with students / 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 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						
Breaching copyright or licensing regulations		X						
Continued infringements of the above, following previous warnings or sanctions		X						

Appendices:

Appendix 1: AUP Reception and Y1

Appendix 2: AUP Y2/3/4

Appendix 3: AUP Y5/6

Appendix 4: AUP Staff, Governors and visitors

Appendix 1: AUP Reception and Year 1

What is this policy for?

This agreement tells you what you can do to keep yourself safe online, and what you must do when using computers, tablets and the internet in school.

The Vision for E-safety

At Crockerne Church of England Primary we seek to build a school community who are able to keep themselves safe and have resilience in an ever-changing digital world. E- Safety is thought of with utmost importance and feeds into our safeguarding provision.

Guidelines

By signing this agreement you are saying that you will follow school rules when using technology in school, and that you will be careful, safe and kind when using the internet out of school.

To stay safe when we use internet

- I will ask an adult if I want to use the computers or tablets
- I will only use activities that an adult has told me I am allowed to use
- I will be gentle with the computers and tablets
- I will not eat or drink near the computers and tablets
- I will ask an adult for help if I am not sure of something
- I will tell an adult if I see something online that I do not like, or something that scares me
- I will search the internet using Google

Name _____ Signed _____ Date

_____

Appendix 2: Year 2/3/4

What is this policy for?

This agreement tells you what you can do to keep yourself safe online, and what you must do when using computers, tablets and the internet in school.

The Vision for E-safety

At Crockerne Church of England Primary we seek to build a school community who are able to keep themselves safe and have resilience in an ever-changing digital world. E-safety is thought of with utmost importance and feeds into our safeguarding provision.

Guidelines

By signing this agreement you are saying that you will follow school rules when using technology in school, and that you will be careful, safe and kind when using the internet out of school.

To stay safe:

- I will be aware of the danger of strangers online, and that not everyone will be who they say they are.
- I will not share personal information about myself or others online (this includes name, address, school, financial details, patterns of activity).
- I will tell a parent or teacher if I do something wrong online, or if I see something I do not like.
- I will not bring my mobile phone or other device into school.

When using the internet:

- I will not open any websites, links or pictures if I do not know what it is.
- I will use Googleas a search engine to ensure that my search is safe.
- I will be polite and responsible online. I will not say anything hurtful or harmful, and will report anyone who does.
- I will always ask for help from an adult if I am unsure of something.

- I will remember that not everything on the internet can be believed.

Photographs and videos:

- I will only take photographs of other people with their permission.
- If I do not want my photo to be taken or used then I can tell someone to stop, or request that it is removed.

Name _____ Signed _____

Date _____

Appendix 3: Year 5/6

What is this policy for?

This policy sets out the acceptable use of technologies by Crockerne Church of England Policy in Years 5 and 6. It intends to ensure that users of technology stay safe while using the internet and other communication technologies for educational, personal and professional use; and that young people become responsible and resilient users of the internet and information technology.

The Vision for E-safety

At Crockerne Church of England we seek to build a school community who are able to keep themselves safe and have resilience in an ever-changing digital world. E-safety is thought of with utmost importance and feeds into our safeguarding provision.

Guidelines

Users will sign to say that they agree to adhere to the acceptable use rules and they understand that school systems must be used in a responsible way, ensuring no risk to school systems, or the identity or safety of other users.

For my personal safety:

- The school will monitor my use of school technology and communications systems.
- I will not disclose my username or password to anyone else, nor will I try to use anyone else's. I will ensure that I maintain strict password security at all times.
- I will be aware of the danger of strangers online, and that not everyone will be who they say they are.
- I will not share personal information about myself or others online (this includes name, address, school, financial details, patterns of activity)
- I will immediately report any illegal, inappropriate or harmful material or incident to a member of staff.
- I will not bring my mobile phone or other device into school without permission from the Co-Headteachers.

- If I chat to someone online I will make sure that a trusted adult (such as a teacher or parent) is aware of this.

When using school technology and sites:

- I will not open any hyperlinks or emails which have come from an unknown source, or any which I am uncertain of.
- I will not use any external memory device without gaining permission from my teacher first.
- I will not share individual passwords and usernames, and will not use another person's to login to any network, website or system.

Use of photographic and video equipment and images

- I will ensure that when I take and/or publish and share images of others I will only do so with their permission.
- Photographs should only be taken for a specific purpose. For example, a project about weather reporting may need photos of people dressed in different clothing, but would not require photos of people making silly faces or doing a dance.
- If I do not want my photo to be taken or used then I can tell someone to stop, or request that it is removed.

When using the internet

- I will use Google as a search engine to ensure that my search is safe.
- I will ensure that I have permission to use the original work of others in my own work.
- I will not download or distribute work protected by copyright.
- When researching, I will be aware that not everything on the internet can be believed, and that information can be false or inaccurate.
- I will be polite and responsible online. I will not say anything hurtful or harmful, and will report anyone who does.
- I am responsible for my own actions, and I will ensure that I have a respectful digital footprint.
- I am aware that any content I put on the internet is there forever and may harm my future chances when applying for jobs and/or further education.

Monitoring and Evaluation

The E- Safety committee will monitor the impact of this agreement and the safeguarding team review online safety incidents and act upon these where necessary.

I understand that if I fail to comply with the agreement, I could be subject to disciplinary action in line with the behaviour policy.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) within these guidelines.

Name _____

Signed _____

Date _____

Appendix 4: AUP Staff, Governors and Visitors

What is this policy for?

This policy sets out the acceptable use of technologies by Crockerne Church of England Primary staff, govenors and volunteers (including students). It intends to ensure that users of technology stay safe while using the internet and other communication technologies for educational, personal and professional use; school systems and users are protected from accidental or deliberate misuse that could put systems at risk; and that staff are protected from potential risk in their use of technology.

The Vision for E- Safety

At Crockerne Church of England Primary we seek to build a school community who are able to keep themselves safe and have resilience in an ever-changing digital world. E-safety is thought of with utmost importance and feeds into our safeguarding provision.

Guidelines

Users will sign to say that they agree to adhere to the acceptable use rules and they understand that school systems must be used in a responsible way, ensuring no risk to school systems, or the identity or safety of other users. Users must also understand that their online presence and digital footprint must reflect their high standards of professionalism and confidentiality.

Rules and security applies to teaching staff using any school system. This includes, but is not limited to, Scomis, Tapestry, Times Tables Rockstars etc.

For my professional and personal safety:

- The school will monitor my use of school technology and communications systems.
- The rules set out in this agreement apply to my use of school hardware and technology both in and out of school.

- School technologies are primarily intended for educational and teaching use. I may occasionally check personal emails, but not during hours of pupil supervision.
- I will not disclose my username or password to anyone else, nor will I try to use anyone else's. I will ensure that I maintain strict password security at all times.
- I will immediately report any illegal, inappropriate or harmful material or incident to the E-safety Lead, DSL or Deputy DSL.
- I will not keep my personal mobile devices in any area frequented by pupils, and will only use it in staff areas during break times.
- Personal mobile devices must not be taken on any school trip or visit unless permission is given by the co-headteachers.

When using school technology and systems:

- I will communicate in a professional manner, not use aggressive or inappropriate language and appreciate that others may have a different opinion.
- I will only use official school social media sites as means to communicate with the community, and to advertise the school in a positive manner. Conversations should not be entered into by staff members through the school pages.
- I will not enter into communication with parents via electronic means, without prior discussion with the head or deputy. Communication with pupils will not be through electronic systems, with the exception of marking feedback on school-wide sites such as Purple Mash.
- I will not engage in any online activity that may compromise my professional responsibilities.

Use of photographic and video equipment and images

- I will ensure that when I take and/or publish images of others I will do so with the express permission of parents.
- Staff should have an open discussion with pupils about the reasons for their photographs being taken, and what will happen to them next.
- Pupils in Years 5 & 6 may be given the opportunity to make their own decisions about photographic and video permissions in certain situations in preparation for the outside world and secondary school. But this would not be that the child could give consent against parental wishes.
- Images should only be taken on school equipment; the personal equipment of staff must not be used for such purposes.
- It is not appropriate for pupils or parents to take informal, 'fun' pictures or videos of teachers and staff where there is no school 'need'. A professional identity must always be of utmost importance.
- Photographs published will be selected carefully and will not include the child's full name.
- Staff must ensure that they are aware of who **does not** have photographic permission, and ensure that these children are safeguarded against a breach of this.
- Staff members are responsible for ensuring that photographs taken by third parties (e.g. another school) meet our guidelines. If unsure, then permission for photographs must be denied.

To ensure the safety of school technologies and systems

- I will not open any hyperlinks in emails or their attachments unless the source is known and trusted, or if I have any concerns about the validity of the email.
- I will ensure that data is regularly backed up and that school devices are used within school on a daily basis to allow for automatic updates to security.
- I will not upload, download, or access any materials with are illegal or inappropriate or may cause harm or distress to others.
- I will not cause damage to, or disable, the equipment of school or other people.
- I will adhere to the rules of the Data Protection Policy with regards to the transportation and storage of data. With this in mind, I will not use any personal device to access personal data of any school users.
- I will immediately report any faults or concerns involving school equipment, software or technologies to the E-safety Lead, or IT technician.

When using the internet in school

- I will check the content of any website or software before using in front of pupils.
- I will ensure that I have permission to use the original work of others in my own work.
- I will not download or distribute work protected by copyright.

Monitoring and Evaluation

The E-safety committee will monitor the impact of this agreement and with the safeguarding team review online safety incidents and act upon these where necessary.

I understand that if I fail to comply with the agreement, I could be subject to disciplinary action in line with the staff disciplinary policy.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) within these guidelines.

Staff/volunteer name _____

Signed _____

Date _____