CIRENCESTER KINGSHILL SCHOOL

E-SAFETY POLICY

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. Indeed, one of the key implications of COVID-19 was in the development in our use of remote learning, largely through email and Teams as the primary platforms for our work. The internet, video conferencing facilities and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times. Keeping pupils and teachers safe during remote education is essential.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Many of these risks reflect situations in the off-line world and so it is essential that this E-Safety Policy is read in conjunction with the school's policies on behaviour, anti-bullying, child protection and allegation management.

As with all other risks, it is impossible to eliminate those risks completely. The E-Safety Policy that follows explains how we intend to minimise these risks, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while accessing the internet and other communications technologies for educational, personal and recreational use.

In reference to Keeping Children Safe in Education, 2020 (KCSiE), it is important to recognise the reference to Online Safety in Annex C: Online Safety. It is stated that *'The use of technology has become a significant component of many safeguarding issues…technology often proves the platform that facilitates harm.'* As such, we need to be mindful that with children spending increasing amounts of time using technology to access their work and working in greater isolation than previously, there is potentially greater risk of harm and we need to ensure that we have a clear policy in place that provides guidance to safeguard children and staff and offers guidance to parents and carers.

This policy also incorporates some of the considerations and approaches we adopt following government guidance on Safeguarding and Remote Education during Covid19 (updated Oct. 20), which is reflected in the appendix at the end of this policy and which has been informed in line with the DfE's Coronavirus (COVID-19):Safeguarding in schools, colleges and other provider's guidance (27th March 2020); guidance from Safeguarding in Education, Gloucestershire and Attendance in Education and Early Years Settings During the Coronavirus (COVID-19) Outbreak, updated on 12th January 2021. It has also been informed through reference to a wide range of other bodies, linked to issues around e-safety and also listed in the appendix.

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 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 out of school, but are linked to membership of the school.

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.

Monitoring of the Policy

The school will monitor the impact of this policy using:

- logs of reported incidents
- internal monitoring data, including internet activity

Roles and Responsibilities

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

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 Chairs Committee receiving regular information about e-safety incidents and monitoring reports annually, to be discussed at the meeting

in Term 1. The Chair of Governors will take on the role of ***E-Safety Governor***. The role of the E-Safety Governor will include:

- annual meetings with the E-Safety Coordinator
- discussion of the impact of monitoring and filtering software, including review of incident logs as appropriate
- annual reporting to the Governor's Curriculum and Pastoral Committee.

Headteacher and Senior Leaders:

- The Headteacher is responsible 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 Coordinator.
- The Headteacher and another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see flow chart on page 11).

E-Safety Coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- liaises with school ICT technical staff
- receives reports of e-safety incidents from the Network Manager and oversees a record of incidents to inform future e-safety developments

- meets annually with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team.

Network Manager:

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and not open to misuse or malicious attack
- that, where necessary the infrastructure is developed to take into account the need to ensure safe usage of new technologies
- that the school meets required e-safety technical requirements and any Local Authority / other relevant 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
- South West Grid for Learning (SWGfL) is informed of issues relating to the filtering applied by the Grid
- the school's filtering is applied and updated on a regular basis and in line with SWGfL guidance
- that The Network Manager keeps up to date with e-safety technical information in order to effectively carry out his e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Coordinator
- that monitoring software / systems are implemented and updated as agreed in school policies
- that any new technologies used in school are reviewed for safe usage.

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 school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Coordinator
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and ensure that processes are followed for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead:

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

- sharing of personal data

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

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

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to read and sign on entry to the school
- 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 to a member of staff
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents and 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 help parents and carers understand these issues through its website and parents' forums. Parents and carers will be encouraged to support the school in promoting good e-safety practice and by endorsing (by signature) the Pupil Acceptable Use Policy and returning this with admission forms.

Policy Statements

Education – pupils

E-Safety education will be provided in the following ways:

- A planned e-safety programme as part of ICT / Personal Social Health and Economical Education (PSHEE) – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- We have provided – and will continue to provide – Parent Forums to promote parental understanding of the issues related to e-safety and keeping children safe.
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in searches being blocked. In such a situation, teachers can request that the Network Manager temporarily

removes these sites from the filtered list for the period of study. Any requests to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

The school will provide information and awareness to parents and carers through its website and parents' forums.

Education & Training – Staff

- A planned programme of e-safety training will be made available to staff.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies.
- The E-Safety Coordinator (through the Network Manager) will receive regular updates through attendance at relevant training sessions 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.

Training – Governors

Governors should take part in e-safety training if they are regular users of the school network.

Technical – infrastructure / equipment, filtering and monitoring

The school is 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.

- School ICT 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 ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager.
- All users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager will be available to the E-Safety Coordinator and kept in a secure place (e.g. school safe).
- Users will be made responsible for the security of their username and password.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Users will report any actual / potential e-safety incident to the Network Manager or E-Safety Coordinator.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- "Guests" (e.g. trainee teachers, visitors) on the school system will be asked to sign a copy of the Staff and Volunteer Acceptable Use Policy Agreement if they are provided with unsupervised access.
- An agreed policy is in place regarding the downloading of executable files by users.

- Programmes should not be installed by staff on school workstations / portable devices whilst in the 'school domain'.
- Personal data cannot be sent over the internet or taken off the school site on removable media (e.g. memory sticks / CDs / DVDs) unless safely encrypted or otherwise secured.

Use of digital and video images - Photographic, Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioners Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff 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. These images should only be stored on school equipment.
- 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

General Data Protection Regulation

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational

measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data Protection Officer – Darren Stillman
Data Protection Co-ordinator – Duncan Evans

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.
- Hard copies of data to be stored securely and shredded when no longer needed.

When personal data is stored on a USB stick or any other removable media:

- the data must be encrypted and/or password protected (Network Manager to supply staff with USB sticks with this facility)
- the device or any data that comes under data protection must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Secure transfer of data and access out of school

Cirencester Kingshill School recognises that personal data may be accessed by users out of school, or transferred to other agencies via secure means. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software and particular care should be taken if data is taken or transferred to another country.

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:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	/				/			
Use of mobile phones in lessons				/				/
Use of mobile phones in social time		/					/	
Taking photos on mobile phones or other camera devices		/					/	
Use of personal iPads and tablets	/							/
iWatches and other smart watches	/				/			
Use of messaging/internet/social media features on iwatches during the school day			/					/
Checking of personal email addresses in school on the school network		/					/	
Use of school email for personal emails		/					/	
Use of social networking sites		/					/	
Use of blogs	/				/			

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

- The official school email service may be regarded as safe and secure and is monitored. 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 need to be aware that email communications may be monitored.
- Users must immediately report 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. Pupils should report this to a member of staff; staff should report this to the Network Manager or the E-Safety Coordinator.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on

official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for students 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 students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to students, 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.
- 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 Data Manager to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Appropriate and Inappropriate Use by Staff or Adults

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff should receive a copy of the E-Safety Policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the school, to keep under file with a signed copy returned to the member of staff.

The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

When accessing the Learning Platform from home, the same Acceptable Use Agreement will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher / Designated Safeguarding Lead immediately and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Appropriate and Inappropriate Use by Children or Young People:

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

School should encourage parents / carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school/education setting or other establishment that the agreement are accepted by the child or young person with the support of the parent / carer. This is also intended to provide support and information to parents / carers when children and young people may be using the Internet beyond school/education setting or other establishment.

Further to this, it is hoped that parents / carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents / carers feel should be addressed, as appropriate. The downloading of materials, for example, music files and photographs need to be appropriate and ‘fit for purpose’ based on research for work and be copyright free.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by some schools of pupils bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD as well as insurance implications in the event of damage. Use of BYOD risks vulnerabilities in an existing secure environment and for this reason, we do not permit pupils to bring their own laptops/tablets for use in school.

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 should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

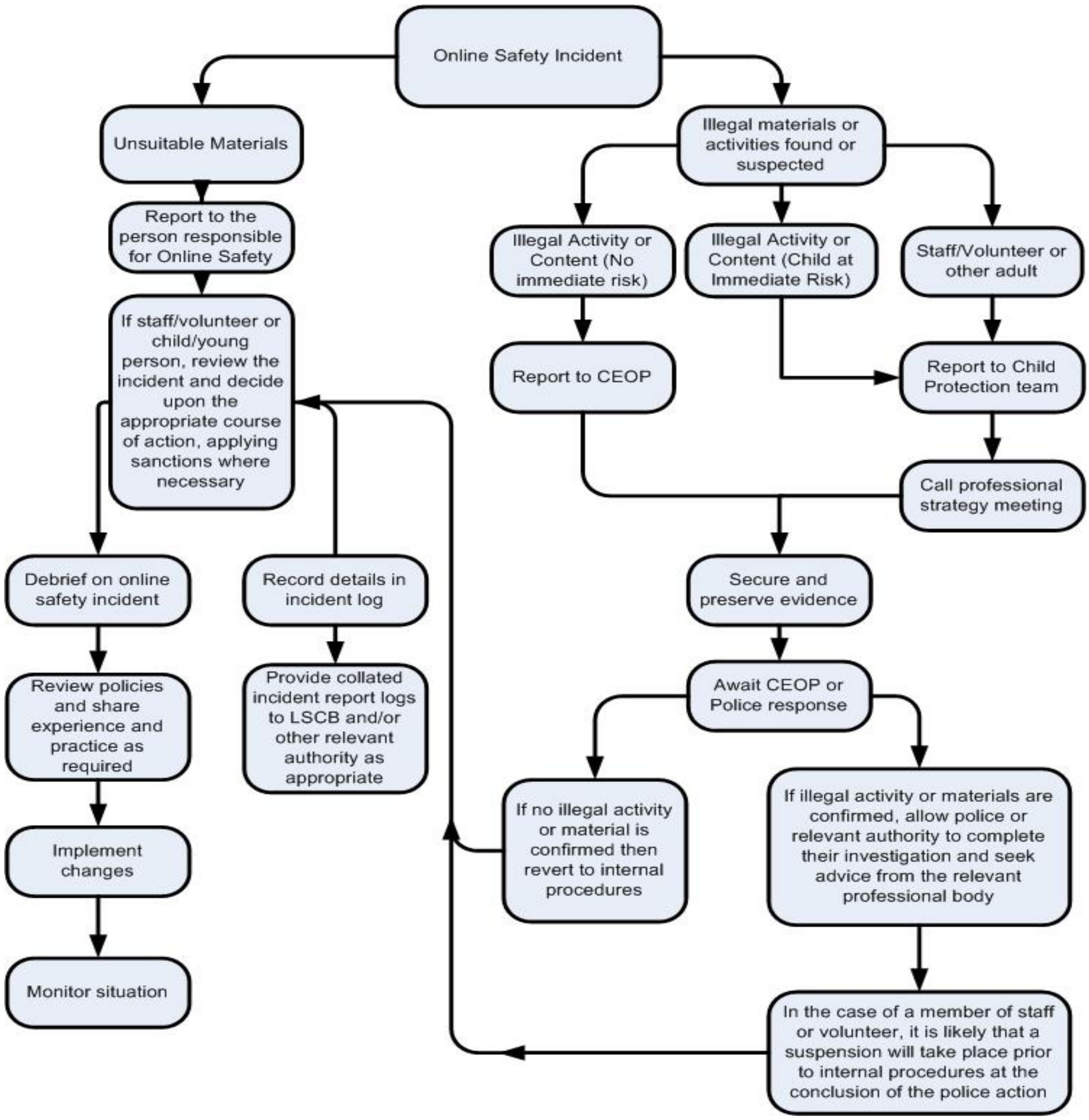
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					/
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					/
	adult material that potentially breaches the Obscene Publications Act in the UK					/
	criminally racist material in UK					/
	pornography				/	
	promotion of any kind of discrimination				/	
	promotion of racial or religious hatred				/	
	threatening behaviour, including promotion of physical violence or mental harm				/	
	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				/	
Using school systems to run a private business					/	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					/	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					/	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					/	
Creating or propagating computer viruses or other harmful files					/	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					/	
On-line gaming (educational)		/				
On-line gaming (non educational)					/	
On-line gambling					/	

On-line shopping / commerce				/	
Peer-to-peer file sharing				/	
Use of social networking sites				/	
Use of video broadcasting e.g. Youtube		/			

Responding to incidents of misuse

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 will 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 School Senior Leadership 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 and the Gloucestershire Safeguarding Children Board (GSCB). Other instances to report to the police would include:**
  - Police involvement and/or action
  - 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.

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

Pupils:

a) Serious incidents should be referred to the appropriate Head of Key Stage who will take the appropriate action. Serious incidents include:
   - Attempting to access or accessing the school network, using the account of a member of staff.
   - Corrupting or destroying the data of other users.
   - Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature.
   - Using proxy sites or other means to subvert the school's filtering system.

- Accidentally accessing offensive or pornographic material and failing to report the incident.
- Deliberately accessing or trying to access offensive or pornographic material.

b) Minor incidents will be dealt with by subject staff in the following ways:

   i. First offence: Faculty detention.
   ii. Second offence: Senior detention.
   iii. Third offence: Refer to Head of Year for possible short term ban.

Minor incidents include:

- Unauthorised use of non-educational sites during lessons.
- Unauthorised use of social networking / instant messaging / personal email.
- Unauthorised downloading or uploading of files.
- Allowing others to access school network, using another pupil’s account.
- Sending an email on the school’s system to a friend containing inappropriate language.

c) Unauthorised use of mobile phone
Action:

- First offence in a term – item confiscated by teacher; Upper / Lower School detention set by Head of Year.
- Second offence in a term – item confiscated by teacher; Senior detention set by Head of Year.
- Further offences in a term should be referred to the appropriate Head of Key Stage.

d) Use of smart watches
It is recognised that more and more members of the school community now wear smart watches. It has been agreed that it is very hard to differentiate between occasions when a pupil may be checking their watch for the time or other uses such as reading text messages. Staff are asked to be vigilant and report any obvious misuse of a smart watch to the pupils Head of Year or Head of Key Stage so further action can be followed up on. In repeated cases, this may include sanctions including detentions and/or confiscation of either the watch or the mobile phone.

Staff

Any suspected misuse by staff should be reported to the Headteacher at the earliest opportunity and will be the subject of a disciplinary investigation and appropriate action taken.

THIS POLICY SHOULD BE READ IN CONJUNCTION WITH THE ACCESSIBILITY PLAN, ANTI-BULLYING POLICY, SCHOOL DISCIPLINE AND BEHAVIOUR POLICY, CHILD PROTECTION POLICY, LOOKED AFTER CHILDREN POLICY, EQUALITY POLICY, EXCLUSION POLICY, OFFENSIVE WEAPONS POLICY, SUBSTANCE MISUSE POLICY, GDPR POLICY THE FAIR PROCESSING NOTICE (FREEDOM OF INFORMATION) POLICY.

Annex to E-Safety Policy, in view of Remote Learning during periods of school closure, written January 2021

Approved by: Curriculum and Pastoral Governors, Andy Johnson and Maureen Richards on 22nd January 2021

1. Live Lessons

At Cirencester Kingshill School, we provide remote education using Microsoft Teams which laregly follows pupils' usual school timetable. Based on guidance from the UK Safer Internet Centre on safe remote learning, staff are aware that teaching from home is different from teaching in the classroom. Similarly, pupils (and their parents) know that learning from home is different to learning in the classroom. Teachers and pupils are encouraged to find a quiet or private room or area to engage in the educational process and are asked to note the guidance offered below.

2. Guidance for Staff: Remote Learning

- Teachers are asked that when delivering their sessions, they remind pupils of the need for appropriate conduct.
- Teams lessons are recorded, both to provide access at a later time for any pupils who may have missed the session or wish to review it, and also, if necessary, to ensure there is a record of anything that may be classed as inappropriate within our usual Behaviour Policy.
- An attendance record should be completed with issues around non-attendance followed up through communication with the pupil, parent, HoY and HOF, as appropriate.
- Teachers are asked to ensure that when delivering their sessions, they are professionally dressed and in a suitable workspace, remembering that this is visible to pupils. Background filters may be used to help achieve this.
- If online assessments are issued, it is important for teachers to reinforce the fact that these should be carried out independently and do what they can to reinforce the school guidelines.
- Teachers will contact parents and pupils where they are not accessing their Teams lessons and will inform Heads of Year if the situation does not improve.

3. Guidance for Staff: Communicating with Parents, Carers and Pupils

Whilst education is taking place remotely due to coronavirus (COVID-19), we must all ensure that we maintain professional practice as much as possible. When communicating online with parents and pupils, it is advised that staff should:

- communicate within school hours as much as possible
- communicate through the school channels approved by the senior leadership team, specifically email and the Show My Homework platform
- use school email accounts (not personal ones)
- use school devices over personal devices wherever possible
- do not share personal information

- Pupils will have weekly contact with both their Head of Year and Tutor. They will also receive updates regarding useful support services e.g. Teens in Crisis+ and how to access this.
- For pupils on the SEND register (regardless of whether they are in school or not), a key worker will make at least weekly contact, in a few cases this may be daily contact. This and any feedback including concerns raised, will be logged.
- The contact details of the DSL and Deputy are on the school web site so parents can contact should the need arise.
- Staff are also reminded of the need to take care not to share contact details when emailing multiple people and being careful when sharing usernames or other log-in details.

4. Providing Remote Pastoral Care

We are still able to provide a level of pastoral care remotely and as a school, maintain high levels of contact with pupils beyond the Teams lesson through weekly tutor sessions and Head of Year assemblies. We will ensure that every pupil has contact information for key members of staff so they know they can raise any concerns. This message is emphasised with pupils and with their parents through the Head's communication, Head of Year assemblies and tutor sessions run on Teams.

As well as this, staff within the pastoral and SEND teams act as key workers for our most vulnerable pupils, maintaining at least weekly contact. All staff are reminded that if calling a parent or pupil from their own phone, they should use 141 to withhold their number. It is preferable to call the pupil's home landline number or their parent's mobile number to speak directly to a pupil, but in the current time, we recognise that there are times when the parent may not be at home and there may not be a home landlne so there may be ocasions where a member of staff makes direct call to a pupil's mobile phone: this should always be done with the parent's permission.

5. Guidance for Pupils: Remote Learning

Whilst education is taking place remotely due to coronavirus (COVID-19), we must all ensure that, as well as making sure pupils keep up with their learning, they stay as safe as possible and adhere to the usual school expectations around appropriate behaviour. Guidelines to support their safety and to reinforce our expectations around pupils' conduct are outlined below.

- Pupils should try to maintain some structure to their day, following their usual school timetable through Microsoft Teams, as outlined above.
- They should also routinely check their school email and Show My Homework to keep themselves updated on communication from teachers and work that has been set.
- They should ensure that when accessing their lessons through Microsoft Teams, their cameras are turned off and they are on mute, unless requested to speak.
- Pupils must not record or take photos of classmates or teachers during Teams lessons, nor share lessons publicly.
- Pupils are advised not to forward any content within a Teams group – such as worksheets, examination papers, answers, solutions, videos, notes or links – to anyone else without the permission of the creator of that content.
- When encouraged to respond either through speaking or through using the Chat bar, they should do so: logging into the lesson in itself should not be the limit of their engagement!
- Pupils should complete the work that has been set and, if requested, send it into to their teacher, either through email or Show My Homework
- Pupils must remember that, despite being at home, a live lesson is an extension of the classroom and pupils should conduct themselves as they would at school. They should be responsible for their behaviour and actions when online, including ensuring that anything they type in the Chat bar is

appropriate and not liable to offend anyone else. They should always be polite and respectful to their teachers and fellow pupils.
- Pupils should understand that these rules are designed to help keep them safe online and that if they are not followed, school sanctions, where possible and appropriate, will be applied and parents contacted.
- If a pupil comes across offensive material they should report it immediately to their teacher or parent.
- Pupils are asked to communicate to staff through either Show My Homework, Microsoft Teams Chat facility or their school email account. They should not use any other email account for communicating with staff.
- Pupils should understand that all online activity is monitored. This includes anything on e-mail and in the Teams lessons.

6. Guidance for Parents, Supporting Engagement and Appropriate Conduct of your Child

- You should ensure that your child is checking in regularly for assigned work.
- When your child is watching a live lesson, you should try to ensure your child is in an area of the house that is quiet and free from distractions.
- It is important to remind children of their conduct online. As a member of Cirencester Kingshill School, they share a digital environment and their behaviour impacts the success of the online school community. Pupils must always follow the direction of their teacher just as in the classroom.
- Parents, pupils and staff are reminded that Microsoft Teams includes a chat function. It is important to note that this facility is monitored and sessions are recorded: pupils must be aware of the need to ensure that any chat is appropriate and not in any way, abusive or offensive to others.
- We would insist that students do not try to film the session using any device.
- Pupils are not to turn on their microphone unless the teacher invites them to do so. All microphones should be on mute when a person is not speaking to avoid distracting background noise being broadcast to other participants.
- A live online lesson must be treated like a regular school lesson and only viewed by those who are invited to attend. The teacher will decide who should receive the invite through Teams. Only those invited by the teacher have permission to view the lesson.
- Cirencester Kingshill School does not expect any child to sign up to anything with a personal email address. They should either use their school email address or a username and password.
- Parents are asked to ensure that their child always keeps their login to both email and any educational software packages private and that they don’t share their account with anyone.
- If online assessments are issued, it is important for parents to reinforce the fact that these should be carried out independently and do what they can to reinforce the school guidelines.

7. Online Risks

With all young people using the internet more during this period, we are aware of the signs and signals of cyberbullying and other risks online and as a school, we apply the same child-centred safeguarding practices as when children are learning in the school.

- The school continues to ensure appropriate filters and monitors are in place
- Our governing body will review arrangements to ensure they remain appropriate
- The school has taken on board guidance from the UK Safer Internet Centre on safe remote learning and guidance for safer working practice from the Safer Recruitment Consortium.
- Staff are reminded that professional boundaries must not slip during these unusual times and are reminded of the school’s code of conduct and importance of using school systems to communicate with children and their families.
- Children and young people receive appropriate guidance on issues related to remote learning.

- Parents and carers have information via the website about keeping children safe online with peers, the school, other education offers they may access and the wider internet community. Parents may find the links in the appendix helpful.

8. Safety Considerations for Parents (based on advice from Nationalonlinesafety.com and the schoolbeat officer)

Secure online chats and chatrooms

It is normal for students to want to be able to communicate with each other whilst they are unable to see each other. It will help them feel less isolated and they will be able to help each other out with their home learning. When online, a child may also make use of chatrooms to get help on their work or to find someone to talk to. However, it is crucial that they can do this safely and there are also some risks associated with them, so it's important to reiterate general online safety advice around using messaging apps and chatrooms.

- Advise children to never give out personal information about themselves, friends or family online and always think before answering private messages.
- Ensure that your children don't put unnecessary personal information in the user profile of any apps that are installed for either educational or recreational purposes. For example, try to keep location, phone number and dates of birth private
- Some online 'friends' are actually just strangers and children should not hesitate to block people that make them feel uncomfortable. They should take a screenshot of their conversation if they need to report the conversation to someone.
- Children can always log out to avoid unwelcome situations or change their screen name if necessary. Children should never use their real name in a chatroom and should report any users who are breaking the rules set out by the chatroom provider.
- The best messaging apps will use encryption while transmitting the data, so that it can't be intercepted and read by others. Many have end-to-end encryption to protect messages along with other forms of communication, such as group chats, voice calls, media files etc.
- To ensure that there are no security flaws in any applications that children are using, make sure they are also kept up to date and install any patches as soon as they become available. Always check the terms and conditions of any applications that are being used, especially those around age. For example, by default, Skype restricts the privacy settings of users under 16 years old. However, this won't be effective if they are registered with parental information
- Help to educate your child on how to use these programs to ensure they are safe. Careless use of any technology can lead to a breach of personal security, downloading viruses or malware or even contact from people they don't know.
- Remind your child to never accept instant messages, phone calls, screen sharing or files from someone they don't know.
- Consider using a parental control tool like Skypito to manage who your children communicate with. Skypito requires parents to approve all of their child's Skype contacts, and allows them to restrict calls and chats with strangers.

TikTok

Like many other Social Media platforms, TikTok has an age restriction of 13 years old. Whilst TikTok can be very appealing to younger audiences, many parents and carers are reminding their children that they need to be 13 before having the app.
Some parents and children have reported inappropriate content on the app, others have raised concerns about the risks linked to the messaging function and children keeping profiles open in order to get more comments and shares.
In the Appendix is the link to a Panorama episode which looked into how safe TikTok really is.

Protecting your home network

It is important to make sure that your home network is secure. Increased use of the Internet for anything increases your risk of clicking on or downloading something nasty to your network, so it's important you have anti-virus / anti-malware software installed to ensure the safety of your family.

- Keep your anti-virus program updated daily and allow it to stay current. There are new attacks every day and the amount of malicious content on web applications is rapidly increasing in both frequency and expertise so it's important to stay up to date.
- If you have a wireless router, check that your wireless network is secure so that people living nearby can't access it. It is best to set up your network so that only people with a wireless 'key' (i.e. password) can connect to your network.
- If your network is secure, users will be prompted for a password when they try to access it for the first time and there should be a padlock symbol next to the network name. If this doesn't happen, your network isn't protected and anyone will be able to join.
- It is always best to change the name of your network from that which was originally provided – but not to anything that identifies it to you or your family. You should also change the default password, as these are often freely available to attackers online if they know where to look. You should choose a password of at least 8 characters, with a mix of case, numbers and symbols. The current advice is to pick three random words or a memorable phrase.
- Always cross-check information if you're not sure about what your child is being asked to do and speak to the school contact.

9. Reporting concerns

It is essential to have clear reporting routes so that children, teachers, parents and carers can raise any safeguarding concerns in relation to remote online education.
The school's safeguarding procedures continue in line with our Child Protection Policy.
The Designated Safeguarding Lead is: Debbie Christopher: dchristopher@cirencesterkingshill.gloucs.sch.uk
Tel: 01285 651511
The Deputy DSL is: Jeremy Morland: jmorland@cirencesterkingshill.gloucs.sch.uk Tel: 01285 651511
The school's approach ensures the DSL or a deputy is always contactable while the school is open. All staff will be re-issued with contact details for the DSL's during school closure and should report any concerns via email or telephone Mrs Christopher direct. *A member of SLT will be on site at all times while school closures are in operation.*

Staff will continue to follow the Child Protection procedure and advise the safeguarding leads immediately about concerns they have about any child, whether in school or not. COVID-19 means a need for increased vigilance due to the pressures on services, families and young people, rather than a reduction in our standards.

In addition to this, teachers, pupils, parents and carers can be referred to the practical support that's available for reporting harmful or upsetting content as well as bullying and online abuse, as outlined below and in the appendix.

Harmful or upsetting content

- reporting harmful online content to the UK Safer Internet Centre
- getting government advice and trusted resources from Educate Against Hate on safeguarding from radicalisation, building resilience to extremism, and promoting shared values

Bullying or abuse online

- get advice on reporting online abuse from the National Crime Agency's Child Exploitation and Online Protection command
- get advice and support from Anti-Bullying Alliance for children who are being bullied

Personal data and GDPR

As a school, we continue to follow our GDPR policy to inform our approach to data protection. This is available on the school website at: https://www.cirencesterkingshill.gloucs.sch.uk/assets/Policies/2019/Data-Protection-Policy.pdf:

In the event of any concerns or breaches of data protection, these should be reported to:

- Mr Darren Stillman, Data Protection Officer: dstillman@cirencesterkingshill.gloucs.sch.uk
- Mr Duncan Evans, Data Protection Manager: devans@cirencesterkingshill.gloucs.sch.uk

In the context of online learning, it is important to emphasise the following points:

- Personal information including specific pupil progress information will not be shared with others in online lessons/forums.
- We will seek consent for any use of pupils personal information, including photographs/videos for marketing or promotional services.
- Staff are asked to take care to not share contact details when emailing multiple people.
- Staff and pupils are asked to take care when sharing usernames and other personal data for access

Staff, Pupils and Parents/Carers are also advised that information we retain includes:

- Login activity, specifically, the last time a student logged in to their email, Microsoft Teams/Show My Homework account.
- Within Teams, the date and time of if/when a pupil views any assignments or/and when they submit any work that is set
- This is to assist us in making sure pupils are engaging in learning sufficiently and so that we can generate appropriate and relevant feedback to pupils/parents/carers.

Appendix/References: Safeguarding pupils and teachers online

Support for School Staff on e-safety in the context of remote learning:

- remote education advice from The Key for School Leaders
- advice from NSPCC on undertaking remote education safely
- guidance from the UK Safer Internet Centre on remote education
- Schools can access the free Professionals Online Safety Helpline which supports the online safeguarding of both children and professionals. Call 0344 381 4772 or email helpline@saferinternet.org.uk. The helpline is open from Monday to Friday from 10am to 4pm.
- Guidance on teaching online safety in schools provides information to help schools ensure their pupils understand how to stay safe and behave online.

Support for Parents/Carers on e-safety in the context of remote learning:

- support for parents and carers to keep children safe online, which outlines resources to help keep children safe from different risks online and where to go to find support and advice
- guidance on staying safe online which includes information on security and privacy settings
- Thinkuknow provides advice from the National Crime Agency (NCA) on staying safe online
- Parent info is a collaboration between Parentzone and the NCA providing support and guidance for parents from leading experts and organisations
- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Internet matters provides age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- London Grid for Learning has support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Net-aware has support for parents and carers from the NSPCC, including a guide to social networks, apps and games
- Let’s Talk About It has advice for parents and carers to keep children safe from online radicalisation

- UK Safer Internet Centre has tips, advice, guides and other resources to help keep children safe online, including parental controls offered by home internet providers and safety tools on social networks and other online services
- https://www.bbc.co.uk/iplayer/episode/m000p3p9/panorama-is-tiktok-safe Footage from a Panorama documentary, reviewing the use of TikTok by teenagers.
- Reporting to CEOP video (thinkuknow.co.uk)
- Internet matters - for support for parents and carers to keep their children safe online
- South West Grid for Learning - for support for parents and carers to keep their children safe online

CIRENCESTER KINGSHILL SCHOOL

E-SAFETY POLICY

Reviewed by J Morland (E-Safety Coordinator)_________June 2022________ (Date)

Adopted by Governors __________________________________ (Sign) __________________ (Date)

Review date __________June 2023__________

E-Safety Coordinator – Mr J Morland

Network Manager – Mr D Evans

Designated Safeguarding Lead – Mrs D Christopher