KINGS'

SCHOOL · WINCHESTER

Online Safety Policy

Policy Reviewed by:	JCK	December 2022
Approved by:	Education Committee	January 2023
Endorsed by:	FGB	February 2023
To be Reviewed	3 Yearly	February 2026

1. Scope of the Policy

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

1.2 This policy must be read and understood alongside the school's Safeguarding Policy.
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. 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 Online Safety behaviour that take place out of school.

2. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

2.1 Governors:
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors' Education Committee receiving regular information about online safety incidents and monitoring reports.

2.2 Headteacher and Senior Leaders:

- The Headteacher has 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 DSL alongside the Whole School IT Lead.
- The Head teacher, Deputy Head teacher and DSL receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious 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 HR / other relevant body disciplinary procedures).

- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

2.3 Whole School IT Lead:

- Alongside the DSL, takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy / documents
- Alongside the DSL, ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provides training and advice for staff
- Liaises with school technical staff
- Attends relevant Governor meetings
- Reports regularly to Senior Leadership Team
- Creates and implements a Whole School ICT Plan
- Leads innovation in the use of new technologies within classrooms
- Chairs BISCUIT/Strategic Group
- liaises with SLT over the ICT Budget
- Monitors and reviews the ICT Managed Service contract (including canvassing staff for feedback)
- Attends ICT Performance Management Review Meetings with SLT
- Presents ICT initiatives to SLT and other key users/stakeholders in school
- Visits and liaises with other schools in order to share good practice and expertise
- Develops and promotes ICT Training in school
- Reviews Policies relating to ICT/Acceptable Use/ Online Safety
- Champions Online Safety
- Liaises with a member of the Senior Leadership Team to ensure safe and successful remote learning should members of the school community need to learn from home. *(See attached Appendix 1 for Remote Leaning guidance)*

2.5 IT Support Manager / Technical staff:

The IT Support Manager/ Technical Staff are 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
- 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 (provided by Coconnect and internally managed by Netsweeper software) 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 / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Whole school IT Lead or proper investigation and subsequent action / sanction
- That monitoring software / systems are implemented and updated.

2.6 Teaching and Support Staff:

School teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- They have read, understood and signed the Staff Acceptable Use Agreement (AUA)
- They report any suspected misuse or problem to the Headteacher, DSL, Data Protection Officer and Whole School IT Lead as appropriate for proper investigation and subsequent action / sanction
- All digital communications with pupils, parents and carers should be on a professional level and only carried out using official school systems
- When working away from a logged on workstation – it is locked
- Staff using mobile devices to check e-mails or access the network must have a complex security code (fingerprint, iris or 6 digit PIN) enabled on the device. School e-mail is only to be used for school business. Staff must not use their personal e-mail to conduct school business
- They have read the Online Safety policy
- Pupils understand and follow the IT Rules and Code of Conduct for Internet use and emails in the pupil handbook
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations as stated in the pupil acceptable use agreement

- 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
- They monitor use of pupils' computers using Impero
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that they understand how to manage any unsuitable material that is found in internet searches through use of Impero and informing the Whole School IT Lead.

3. Staff laptops

- Laptops are issued to all teaching and some support staff. The issued laptop remains school property and should only be used by its designated keeper for school-related tasks.
- School employees issued with laptops do not have any right to privacy as far as the content of school laptops is concerned and so it is absolutely essential that they are NEVER used for purposes inconsistent with the professional standards of school teachers and support staff.
- The school has a range of security software that will automatically detect and report inappropriate material. The school reserves the right to inspect all school computers and devices, including records of internet sites visited, emails and attachments and any material downloaded. Using any school computer or device inappropriately can be a disciplinary offence.
- Staff should treat laptops as they would any other valuable items and ensure that appropriate security measures are taken. Laptops should not be left unattended at school or in vehicles and care should be taken to ensure that any sensitive data is kept secure to meet the requirements of the General Data Protection Regulations. It is the responsibility of the member of staff to take all reasonable steps to prevent unauthorised access to the laptop.
- Staff should not add software to their laptop. Software must not be copied from the laptop to another device without permission from IT Support and the Whole School IT Lead. IT Support will carry out upgrades to software as required. Staff wishing to use subject specific software must liaise with IT Support to ensure that appropriate licences are held.

- Staff will be required to sign for laptops and should be aware that this equipment will be audited regularly and on return to ensure that equipment has been used within the guidelines specified.

4. Passwords

- Passwords must be complex (numbers and mix of symbols, upper and lower case).
- Passwords must not be divulged to others nor should they be kept in a place that someone could find them
- If a member of staff suspects their password has been compromised, they must inform IT Support and the Whole school IT Lead within 24 hours of becoming aware of a potential compromise.

5. Designated Safeguarding Lead (DSL)

DSLs are trained in Online Safety issues and are to be aware of the potential for serious child protection and safeguarding issues that arise from:

- Sharing of sensitive personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Sexting
- Taking / sharing of inappropriate material (images /videos)
- Issues arising from use of Social Media

6. Pupils

- Are responsible for using the school computer equipment in accordance with the IT Rules, IT Code of Conduct and Parent / Pupil Contract contained in the Pupil Handbook.
- 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 the school rules concerning the use of mobile devices and digital cameras.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

7. Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet. computers and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through Internet Safety presentations, signposting using the school website and in routine school communications. Parents and carers will be encouraged to support the school in promoting good online 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 pupil records
- Their children's personal devices in the school

8. Policy Statements

8.1 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 online safety is therefore an essential part of the school's online safety provision. Pupils need the help and support of the school to recognise and avoid online safety risks and build their resilience.
Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages. The online safety curriculum will be provided in the following ways:

- A planned online safety curriculum will be provided as part of BEE (now Computing), Pastoral Curriculum and PHSEE
- Key online safety messages are reinforced as part of a planned programme of assemblies
- Pupils should be taught in all subjects to be critically aware of the materials and 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 IT Rules and IT Code of Conduct and encouraged to adopt safe and responsible use both within and outside school.
- 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 Whole School IT Lead 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.

8.2 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 procedures approved within this policy are implemented.

8.3 School technical systems will be managed to deliver secure and safe use:

- 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
- Access to the school's network systems will be restricted to designated users.
- All users will be provided with a username and secure password by IT Support who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password at regular prescribed intervals.
- The passwords for the school ICT system, including the administrator passwords used by the IT Support staff will be held by School's IT Services Manager and available to the Headteacher.
- IT Support Staff are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by CoConnect and the Netsweeper filtering system.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.

- The school has provided enhanced / differentiated user-level filtering allowing different filtering levels for staff and pupils
- Kings' also utilises monitoring software called Impero. This alerts key staff to users activity whilst using the schools IT equipment and IT system. These alerts are reviewed regularly.
- IT Support staff regularly monitor and record the activity of users on the school network and users are made aware of this in the Acceptable Use Agreement.
- 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 Acceptable Use agreement is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems).
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (Use of USB Memory sticks or other removable media will not be permitted after 1 May 2018 without the written permission of the Whole School IT Lead)

8.4 Use of digital and video images

School 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. 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 eg on social networking sites
- In accordance with guidance from the Information Commissioner's Office, parents and 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 and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- 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, the prospectus or news media
- Pupils' work can only be published with the permission of the pupil and parents or carers

9. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 (to be replaced by the General Data Protection Regulations (GDPR) in May 2018). Detail is contained in the school's Data Protection Policy.

10. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school equipment(eg by remote access)

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school / academy systems. Personal email addresses, text messaging or social media must not be used for these communications. Members of staff who receive inappropriate communications from pupils MUST report them to their line manager immediately.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

11. Social Media - Protecting Professional Identity

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 on social media
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- School staff should ensure that:
- They do not post on social media any content which identifies pupils, parents, carers or staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Any personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

- The school's website and any associated social media for professional purposes will be checked regularly to ensure compliance with the school's policies.

12. Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is not permitted on the school network or computer systems. 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	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	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	

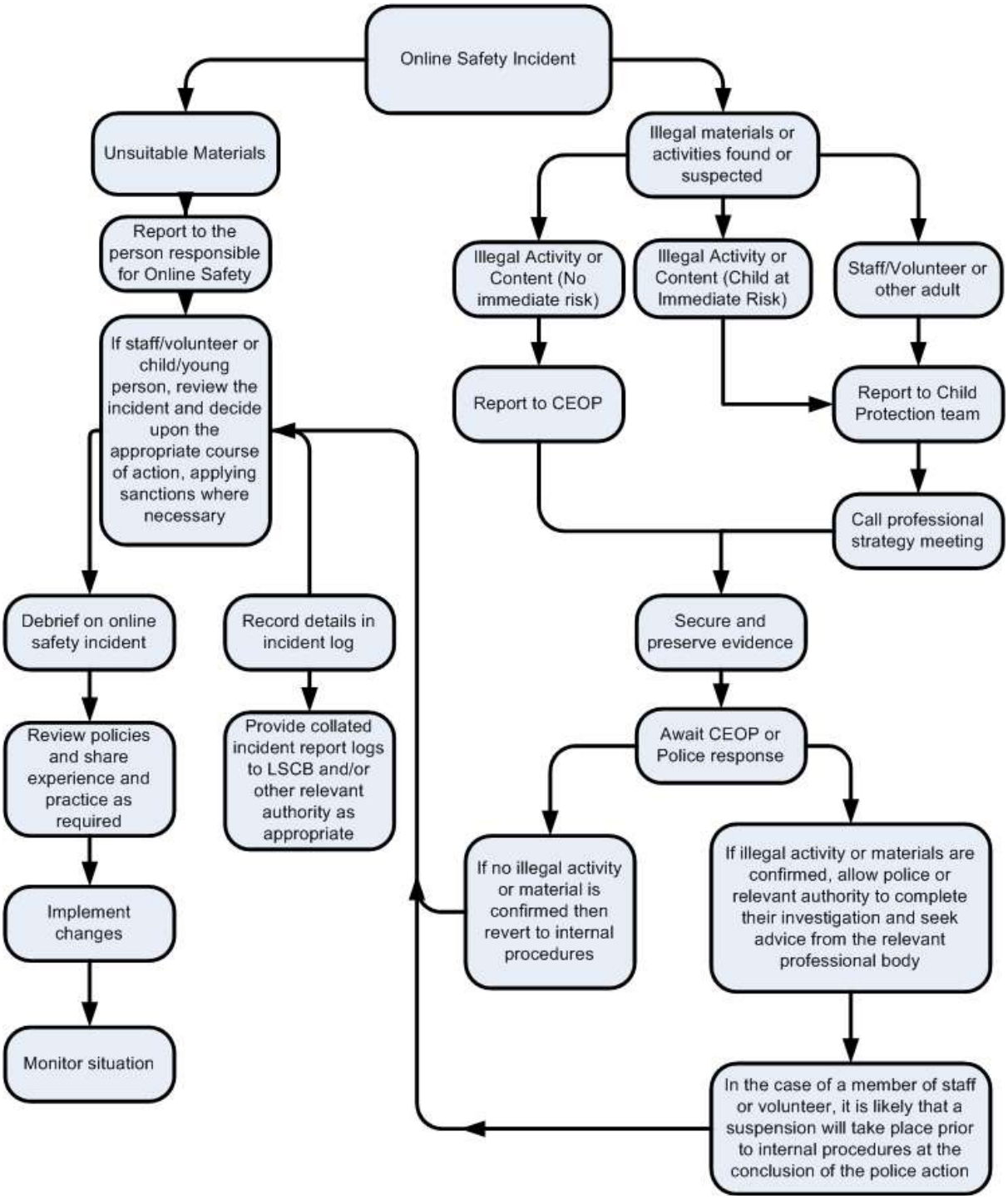
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright						X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			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		

13. Responding to incidents of misuse

In the event of any suspicion that there has been misuse of the school's network or computer systems then the flowchart below should be used to determine the appropriate actions.

13.1 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. If there is any concern about the behaviour of an adult, the Headteacher must also be informed. If the adult is the Headteacher, the Chair of Governors must also be informed.


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

13.2 Other Incidents

Any infringements of this Policy, through careless or irresponsible or deliberate misuse will be investigated using the procedure below:

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

- Have more than one senior member of staff involved in the investigative 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 to the members of staff conducting the investigation.
- 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 investigation report except in the case of illegal content – see below
- Once this has been completed and fully investigated the Headteacher 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
    - Police involvement
- If content being reviewed includes images of Child abuse or other illegal content, 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 or device under investigation. 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.

Appendix 1: Remote Learning – Kings' School

Rationale:

In the event of the school needing to close, the school is committed to provide continued learning for its pupils and will do this through a process of remote (online) learning. This Appendix aims to clarify the school's position if there is an extended period of time when the school is closed. In the event of a short term school closure (e.g. as a result of inclement weather) or for short term pupil absence this Appendix does not normally apply.

Remote learning may also be appropriate in situations when pupils, authorised by the school, have a period of absence but are able to work at home. An example of such a case may be an exclusion from school, or longer term illness, following an infectious disease outbreak, pupils self-isolating but are not suffering from relevant symptoms. There is no obligation for the school to provide continuity of education to pupils who absent themselves from school, with or without parental permission. This may apply, for example, if parents choose to take their son/daughter out of school 'as a precaution' to an outbreak of an infectious disease.

Section 1 – Types of Closure

In the case of partial year group closure

This is where a group of pupils will be asked to self-isolate by the school for a fixed period of time due to coming into close contact with a pupil or pupils that have a positive test for COVID19.

Pupils at home will be expected to attend live lessons as these will be going on in school with the rest of the class. The live lesson that takes place will involve the teacher using the school's preferred platform for delivering lessons e.g. Teams. The teacher will have their microphone enabled in school so that those pupils at home will be able to hear the teacher's explanations and teaching of a particular topic. Lessons will continue at the normal times during the day. There will be a proportion of the lesson time where pupils will be expected to work independently on the task(s) set by the teacher with little/no teacher input.

Please refer to **Section 2** onwards for further clarification about remote learning.

In the case of partial lockdown

This is where one or more-year groups will be working from home. In this instance lessons will continue to take place as normal via the schools preferred online system e.g. Teams. Pupils will be expected to attend these lessons at the normal times from home unless they are unwell. There will

be a proportion of the lesson time where pupils will be expected to work independently on the task(s) set by the teacher with little/no teacher input.

Please refer to **Section 2** onwards for further clarification about remote learning.

In the case of national lockdown

This is where the majority of teaching staff and pupils are not on school site, apart from those attending in order to provide teaching for the children of key workers or those who are deemed vulnerable. Teaching staff will provide live lessons from home using the school's preferred online software e.g. Teams. These lessons will involve the teacher delivering lesson content using a microphone and webcam (if required). Resources used maybe available on the schools SharePoint site and/or Files within the Teams Platform. Pupils would be expected to be online and engaging with the live lesson at the time(s) specified by the school. If a teacher is in school for the purposes of designated keyworker/vulnerable pupils provision, they may either live stream lessons to the rest of the class from their classroom in school or set 'static' lessons for pupils in their class at home. This will allow them to focus on teaching the pupils in the classroom, especially if it is a 'collapsed' class made of pupils from several different timetabled classes.

Please refer to **Section 2** onwards for further clarification about remote learning.

Section 2 – Remote Learning

Remote Learning – What this will look like

If the school closes for an extended period of time the school will provide continuity of education in the following ways: -

- Regular direct instruction from teachers via online lessons. This will be through the use of online platforms agreed by the school e.g. Microsoft Teams, Satchel One platform
- Setting work that pupils will complete- some written responses will be requested electronically in order to assess the pupils' knowledge and relevant feedback given to the pupils.
- The assessment and digital feedback of submitted work will primarily be through Teams and Satchel One but may also be through a department's preferred platform.
- The primary platforms the school will use to deliver continuity of education are: Microsoft Teams: accessed via the desktop application or via the following

URL: www.RMUnify.com or https://teams.microsoft.com, Satchel One (accessed via RMUnify.com) and the school's SharePoint site

The school reserves the right to vary the range of methods used to provide remote learning provision, including delivery, feedback and interaction based on the particular circumstances of any closure.

Practice – Live Lessons

These will take place using the school's preferred platforms such as Microsoft Teams – This is a platform that allows resources to be shared, teachers to 'speak' to pupils and pupils to ask relevant questions in order to clarify their understanding of the content being delivered.
Live sessions can be particularly helpful as they can help communication, with pupils able to respond to teachers' questions (and ask them) via the conversation functionality in teams.

- Pupils are to use their school email address when accessing this, to avoid any issues regarding GDPR, there will be no expectation for parents/carers or pupils to provide their own email addresses for use of the school's system
- Where possible, the teacher leading the lesson or activity may choose to record the lesson so that it can be accessed by pupils at different times
- Recorded lessons remain the property of the school and must not be shared outside of the school community - this includes social media sites or any other forms of broadcasting.
- If a lesson is recorded – the teacher will ensure that only pupils' first names are used
- Pupils and parents/carers are not permitted to film or record lessons in any way unless the teacher or person leading the lesson has given permission for them to do so.
- Serious misuse of online learning opportunities (such as making recordings without permission or, sharing images of adults or other pupils) will be treated under the School's Behaviour Policy and may result in permanent exclusion.
- Links to access the lesson and its content will be sent only to pupils in a teacher's class or specified group and will always be in line with the School's policies for Safeguarding and safe use of IT.
- Any pupil that disrupts or misuses their opportunity to engage with the lesson will be excluded from the group for a fixed period of time until parental and pupil reassurances are given that misuse will not occur in the future
- A recorded lesson does not need to be deleted and may be used again
- Relevant resources may be provided via the schools SharePoint site

- Staff are recommended to use blurred backgrounds at all times, particularly if teaching from home
- Employees of the School reserve the right to seek legal action where a breach of this policy or an act causing harm or potential defamation, takes place.

Assessment of work

Given the nature of the tasks, the type of feedback teachers can provide may not have the same format as marking an exercise book. Teachers are encouraged to ensure, when they set assessed work, that it is designed in such a way that meaningful feedback may be provided.
Under normal circumstances, not all pieces of work are formally assessed by teachers and this would continue to be the case should the school employ remote learning.

Possible methods of feedback may include:

- Providing whole class feedback rather than feedback on individual pieces of work – this is an effective way of providing feedback, supported by findings from educational research
- Using the “Comments” function on online documents or Microsoft
- Sending an email to learners with specific feedback / targets
- Feedback via another website / piece of software such as Satchel One

Pupil Expectations

Pupils that are healthy and well are expected to participate fully in the remote learning provision by attending their relevant live lesson, completing independent work and submitting tasks promptly to the best of their ability. Pupils would also be expected to respond to communication from school regularly – such as their tutor during tutor sessions or their teachers regarding their lessons.

During online live lessons:

- Pupils will be encouraged to respond to teacher input using the 'Chat function' on Teams. The language and behaviour used in this forum should remain polite and respectful to both their peers and members of staff.
- Pupils' cameras should remain off at all times and their microphones muted unless specifically asked to speak by a member of staff.
- If a pupil would like to contribute to a class discussion, they should use the 'hands up' icon on the Teams actions bar to indicate their desire to speak to a member of staff, who will then invite them to speak when appropriate.

- If a pupil's behaviour is deemed inappropriate for the Teams lesson and they have been given a warning, the teacher is able to remove them from the meeting, with the expectation that they catch up on work by accessing the recording of the teacher input for the lesson.

If pupils have questions about specific tasks that have been set, these should be directed to that department area. If there are concerns about the overall workload of the pupil, this should, in the first instance be directed to the department area and then escalated to the Head of Year if the pupil continues to feel overwhelmed.

Teachers will work on the assumption that pupils may not have the full range of books/equipment that they may usually have in school; however, if advanced notice of a school closure is possible, teachers will instruct pupils to take the relevant equipment home with them.

The school expects households to have access to the internet in order to access remote learning materials and that a computer is available for the pupil to use. The school will not expect households to have the ability to print documents. If a household does not have appropriate internet access or technology and they contact the school, the school will undertake to resolve this issue if at all possible.

Expectations of Teachers

Teachers should ensure they have effective internet connectivity at home. If this is not the case teachers may be able to request a school device or, if possible, come to school to use the school's internet connection.

The setting and assessment of remote learning tasks will take place in accordance with school and subject area policies.

In order that teachers are providing a consistent approach, Heads of Department are responsible for overseeing the nature and frequency of tasks set and assessed within their subject areas. All teachers should pay due care to the nature of tasks set, so that pupils have a range of activities to complete at home and are not exclusively working at a computer screen.

Teachers are responsible for providing constructive feedback to their pupils in a timely manner.

If a teacher becomes unwell during a period of remote learning – it is the responsibility of the Head of Department to ensure work is set for that member of staff's classes.

In order to ensure teachers are able to perform the minimum expectations outlined above; the school will provide a range of training opportunities that teachers should access to before any planned school closure. Teachers should ensure that they have looked through specific instructions, watched walkthroughs/documents in the IT training folder on SharePoint and attended teacher training sessions. If teachers require further support with any aspects of remote learning, they are encouraged to consult their BISCUIT member, HOD/S, the IOCT Coordinator or the Senior Leadership team.

Teachers will be expected to be contactable between normal teaching hours 9-3:20 unless there are extenuating circumstances. Members of staff will endeavour to respond to communication within 48hours.

All communication must always be through the school's official communication channels e.g. school email/Satchel One /Teams and not through personal accounts or other websites/apps.

IT Support

The school is not responsible for the setup and functioning of household equipment, however, the school will assist with logging in difficulties for example if a pupil does not know their password/username or needs this resetting.

A parent should email ITHELP@kings-winchester.hants.sch.uk if their son/daughter is experiencing login issues related to their username or password.

Support for pupils with SEND, EAL and other specific learning enhancement needs

Teachers should ensure that work is differentiated as required for all learners when setting online tasks. Profiles are available for SEND pupils and advice can be sought from the SENCO. In addition, the SENCO will maintain contact with identified pupils requiring regular support, by email or phone with parents/pupils.

Pastoral care

In event of a school closure, the primary responsibility for the pastoral care of a pupil rests with their parents / carers. However, tutors (under the guidance of the Head of Year and Senior Leadership

Team) should check in regularly to monitor both academic progress and their general wellbeing. Tutors will be expected to pass on feedback to the Head of Year initially or to the Senior Leadership Team if required, particularly if there are concerns or a lack of communication.

Safeguarding

The school's Child Protection and Safeguarding Policy still applies in the event of a school closure. All interactions between teachers and pupils should be the same as if they were in school. Please refer to the school's safeguarding policy for further information.

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by:

- Designated Safeguarding Lead
- Whole School IT Lead
- Senior Leadership Team
- School Governing Body

The school will monitor the impact of the policy using:

- Monitoring logs of internet and network activity (including sites visited) / filtering / Impero