Keble Prep Online Safety Policy

Development, Monitoring and Review of this Policy

This online safety policy has been developed by a working group consisting of the Headmaster, online safety coordinator (Karen Fleming) and selected staff – including technical staff

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This online safety policy was first approved by the Governing Body	Spring 2015
The implementation of this online safety policy will be monitored by the:	online safety Coordinator Nominated Governor SMT
Monitoring will take place at regular intervals:	Annually
The Education Committee will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The online safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Spring 2020
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Nippy Gecko, Crossover Solutions

The school will monitor the effectiveness of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - pupils
  - parents
  - staff

Scope of the Policy

This policy applies to all members of the Keble School community including staff, pupils, governors, volunteers, parents, visitors, who may be given access to school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headmasters to such extent as is reasonable, to regulate the behaviour of students / 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 cyberbullying, radicalisation or other online safety issues covered by this policy, which may take place away from the school premises, but still linked to membership of the school. The 2011 Education Act increased these powers with regard to searching for, and of, electronic devices and the deletion of data.

The school will deal with such incidents as outlined in this policy and, in conjunction with the associated Behaviour & Discipline and Anti-bullying policies, will inform parents of incidents of inappropriate online safety behaviour that take place out of school when they are known.

Links to Other Policies

This policy is linked to the Behaviour & Discipline Policy, Anti-Bullying Policy, Data Protection Policy, the PREVENT Policy, the Safeguarding Policy and Staff Code of Conduct, the Social Media Policy and the Acceptable Use Policies for Staff, Parents and Pupils.

Roles and Responsibilities

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

Governors

The Governing Board is responsible for the online safety Policy and for reviewing its effectiveness along with the SLT. The formal review will be carried out annually by the Education Committee, which will receive regular information about online safety incidents and monitoring reports.

Mr Justin Scott has taken on the role of online safety Governor

The role of the online safety Governor will include:

- Regular meetings with the online safety Coordinator when needed
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering / change control logs
- reporting to the Education Committee when appropriate

Head Teacher and Senior Leaders:

- The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, through the day to day responsibility for online safety will be delegated to the online safety Coordinator.
- The Head Teacher and (at least) another member of the Senior Management 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 “Responding to Incidents of Misuse” on dealing with online safety incidents in Appendix 1

- The Head Teacher and SLT are responsible for ensuring that the online safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues.
- The Head Teacher and SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Senior Leadership Team will receive termly monitoring reports from the online safety Coordinator.

Online Safety Officer/Lead:

- takes the lead on the management of online safety committee, updating senior managers and others as necessary
- takes day to day responsibility for any online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents taken from Arbor to inform future online safety developments,
- updates annually the online safety Governor with regard to current issues, incident logs and filtering / change control logs
- attends meetings of the Education Committee as necessary
- reports regularly to the Head Teacher and SLT

Director of Digital Learning and Communication *(DoDL)* *(Network manager)*

The Director of Digital Learning and Communication is responsible for ensuring:

- that the technical infrastructure is secure and is not open to misuse or malicious attack
- that the Keble 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 is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that he/she keeps up to date with online safety technical information in order to effectively carry out his/her online safety role and to inform and update others as relevant
- that all aspects of digital use are regularly monitored in order that any misuse or attempted misuse can be reported for investigation and any resultant actions or sanctions
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff
are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headmaster or online safety Coordinator for investigation
- all digital communications with pupils, parents and other members of the community should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, tablets and other mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

The Designated Person (Child Protection Officer)
should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Pupils

- are responsible for using Keble School's digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying

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

Parents

Parents/ carers play a crucial role in ensuring that their children understand the need to use the internet and technology in an appropriate way. The school will take every opportunity to help parents understand these issues. Parents 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 school's online presence
- their son's personal devices in the school

Policy Statements
Delivery

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

Pupils

- A planned online safety curriculum should be provided for pupils as part of ICT, PHSE and other lessons and should be regularly revisited
- Key online safety messages, for example safe electronic contact with strangers or awareness of radicalisation should be reinforced for pupils as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials and content they access online 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 are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models to pupils in their use of digital technologies the internet and mobile devices
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites visited.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Parents

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Keble School will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters and website
- Parents evenings and special meetings with online safety as the core topic for information
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites and publications eg www.swgfl.org.uk www.saferinternet.org.uk or http://www.childnet.com/parents-and-carers

Education & Training

Staff
It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly through the appraisal process.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- The online safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The online safety policy and its updates will be presented to and discussed by staff in staff meetings and/or INSET days.
- The online safety Coordinator will provide advice, guidance and training to individuals as required

Governors
Governors should take part in online safety training or awareness sessions, with particular importance for those who are members involved in online safety, Health and Safety and Safeguarding. This may be offered in a number of ways:

- Attendance at training provided by AGBIS, ISBA, ISI or other relevant organisations
- Participation in school training or information sessions for either staff or parents

Radicalisation

Statutory Duties

The duty to prevent children and young people being radicalised is set out in the following documents.

- Counter Terrorism and Security Act (2015)
- Keeping Children Safe in Education (2019)
- Prevent Duty Guidance (2015)
- Working Together to Safeguard Children (2018)
- Teaching online safety in school (DfE, June 2019)

Non-statutory Guidance

- Promoting fundamental British values as part of SMSC in schools: Departmental advice for maintained schools (DfE 2014)
- The use of social media in online radicalisation (DfE 2015)

Definitions

Extremism is defined in the 2011 Prevent strategy as vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas.

Radicalisation refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

British Values are democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs.

Online Safety

The internet provides children and young people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages.

As a school all the senior boys have 1-1 iPads and each iPad is monitored and all internet activity even at home is redirected through the school filtering system.

The filtering systems used in our school blocks inappropriate content, including extremist content. We also have a further 'white list' of keywords, which will be monitored in addition as part of the filtering process. Any activity on against this white list will be sent to the online safety Officer for further investigation.

We also filter out social media sites, such as Facebook. These are the primary focus for those attempting to radicalise. Searches and web addresses are monitored and the technicians will alert senior staff where there are concerns and prevent further access when newly constructed sites are found.

All emails are monitored for keywords and activity using Google Vault and any suspicious activity is reported by the technicians to the online safety Officer

Where staff, children or visitors find unblocked extremist content they must report it to the school online safety officer.

The Acceptable Use of ICT Policy (AUP) refers to preventing radicalisation and related extremist content. Pupils and staff are asked to sign the AUP annually to confirm they have understood what is acceptable.
Pupils and staff know how to report internet content that is inappropriate or of concern.

Technical – infrastructure, equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the DoDL who will keep an up to date record of these users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every term
- The "master / administrator" passwords for the school's ICT system, must also be available to the Headmaster or DoDL
- the DoDL 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

Mobile Technologies

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

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

· The school Acceptable Use Agreements for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies

The school allows

· The school Acceptable Use Agreements for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes - mobile phones only*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*		*Yes*	*Yes*
Internet only						
No network access						

- Mobile phones are allowed for staff and visitors- boys must hand their phones in at the office each day first thing and are not allowed in classrooms
- Staff and visitors should not use mobile phones in lessons unless it is an emergency or needed for a lesson

Internet Filtering

Internet access is filtered for all users. Illegal content (e.g. images of child sexual abuse) is filtered by the broadband, or filtering provider, by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
In addition: -

- the school provides enhanced / differentiated user-level filtering
- school technical staff regularly monitor and record the activity of users on the school technical systems. Users are made aware of this through the Acceptable Use Agreement.
- an appropriate system is in place for users to report any actual or potential technical incident or security breach to the relevant persons
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts

which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- An agreed protocol is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- agreed protocols are in place regarding the extent of personal use that users (staff, pupils and other users) and their family members are allowed on school devices that may be used out of school.
- A protocol is in place that allows selected staff – and forbids other staff –from downloading executable files and installing programmes on school devices.
- An agreed protocol is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning in allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out Internet searches for information about potential and existing employees. Keble School will inform and educate users about these risks and 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 are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases for safeguarding protection, these images should not be published or made publicly available on social networking sites, nor should parents / carers comment on any activities involving other individuals in the digital images.
- Staff and volunteers are allowed to take digital or video images to support educational aims, but must follow school procedures concerning the sharing, distribution and publication of those images. Staff are allowed to use personal phones or tablets, but must upload all images to the school network and delete images from their personal devices within an appropriate time period.
- 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, when associated with photographs.
- Written permission from parents will be obtained on entry to the school with regard to images of their son being published on the school website
- Pupil's work can only be published digitally with the permission of the pupil and parents. Parents give their permission on entry to the school.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Please see the Data Protection Policy for precise details of the requirements under this legislation.

In terms of digital data the school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes for which it was collected.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA). This control is exercised through the Headmaster, who will also act as the Senior Information Risk Officer (SIRO).
- Information Asset Owners (IAOs) exist for digital data. The bursar (John Field) for financial data, Suzy Tyrrell in the School Office for administrative data and Stella Stringer (as Senco) for Special Needs data. All staff have access to personal data through Arbor and must be mindful of the responsibility to safeguard such data.
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected **devices.**

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

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

	Staff and Adults				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 the school / academy	x							x
Use of mobile phones in lessons			x					x
Use of mobile phones in social time	x							x
Taking photos on mobile phones / cameras	x							x
Use of other mobile devices e.g. tablets, gaming devices	x					x		
Use of personal email addresses in school / academy , or on school / academy network	x						x	
Use of school / academy email for personal emails		x						x
Use of messaging apps		x						x
Use of social media		x						x
Use of blogs		x					x	

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

- The official *kebleprep.co.uk* email service on gmail 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 on school business
- Users must immediately report, to Karen Fleming – 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 (email, chat, Google classroom etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses and social media **must not** be used for these communications Text messaging or social media can be used in some situations - when deemed appropriate and useful - for example using the school's Twitter accounts on school trips or on fixtures to communicate with parents.
- Whole class / group email addresses may be used in the junior school, while pupils in the senior school will be provided with individual school email addresses for educational use.

- 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.

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber bully, discriminate on the grounds of sex, race or disability or who defame a third party may render Keble School liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Keble School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include guidance on acceptable use, social media risks, checking of settings, data protection, etc
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
- Ensuring that personal information is not published

School staff should ensure that:

- No reference should be made in personal social media to pupils, parents or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Their own personal opinions should not be attributed, or construed, to be those of the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The online safety coordinator and online safety committee to ensure compliance with this and other school policies will check the school's use of social media for professional purposes regularly.

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

- A process for approval by senior leaders
- Posts are put by a member of the SLT for the main Keble Prep Twitter account
- Residential trips have locked Twitter accounts are created and lead staff post images and messages from the trip
- If any issues occur any misuse should be reported to the online safety officer

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the Keble Prep

or impacts on the Keble Prep, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

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

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Unsuitable / inappropriate activities

Keble School believes that the activities referred to in the following section would be inappropriate in a school context and that staff users should not engage in these activities in school, or outside school, when using school equipment or systems. The school policy restricts usage as follows:

User Actions			Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not		Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of					X

Children Act 1978					
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	

Also

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		

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 in Appendix 1 for responding to online safety incidents and report immediately to the police.

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by pupils 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).
- Keep a written log of the incident and record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for

investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately.

Other instances to report to the police would include: -

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct activity or materials
- material that is intended to radicalise

In such cases 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 group, for evidence and reference purposes, should retain the completed written log securely.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures and if necessary the school/DSL will contact Enfield Borough council for advice and support if needed.

	Actions / Sanctions								
Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X					
Unauthorised use of non-educational sites during lessons	X								
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X							
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X	X		X				
Unauthorised downloading or uploading of files	X	X							
Allowing others to access school / academy network by sharing username and passwords	X	X							

Allowing others to access school / academy network by sharing username and passwords	X	X							
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X	X	X		X				
Attempting to access or accessing the school / academy network, using the account of a member of staff	X	X	X		X	X	X	X	X

Corrupting or destroying the data of other users	X	X	X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X	X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X						

Accidentally accessing offensive or pornographic material and failing to report the incident	X	X							
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X	X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X							

Staff Incidents	Actions / Sanctions							
	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	X							
Unauthorised downloading or uploading of files	X							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X			X		X	
Deliberate actions to breach data protection or network security rules	X	X						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X		X			X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X						X
Actions which could compromise the staff member's professional standing	X	X						X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X	X						X

Using proxy sites or other means to subvert the school's / academy's filtering system	X				X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X							
Deliberately accessing or trying to access offensive or pornographic material	X	X						X
Breaching copyright or licensing regulations	X							
Continued infringements of the above, following previous warnings or sanctions	X	X					X	

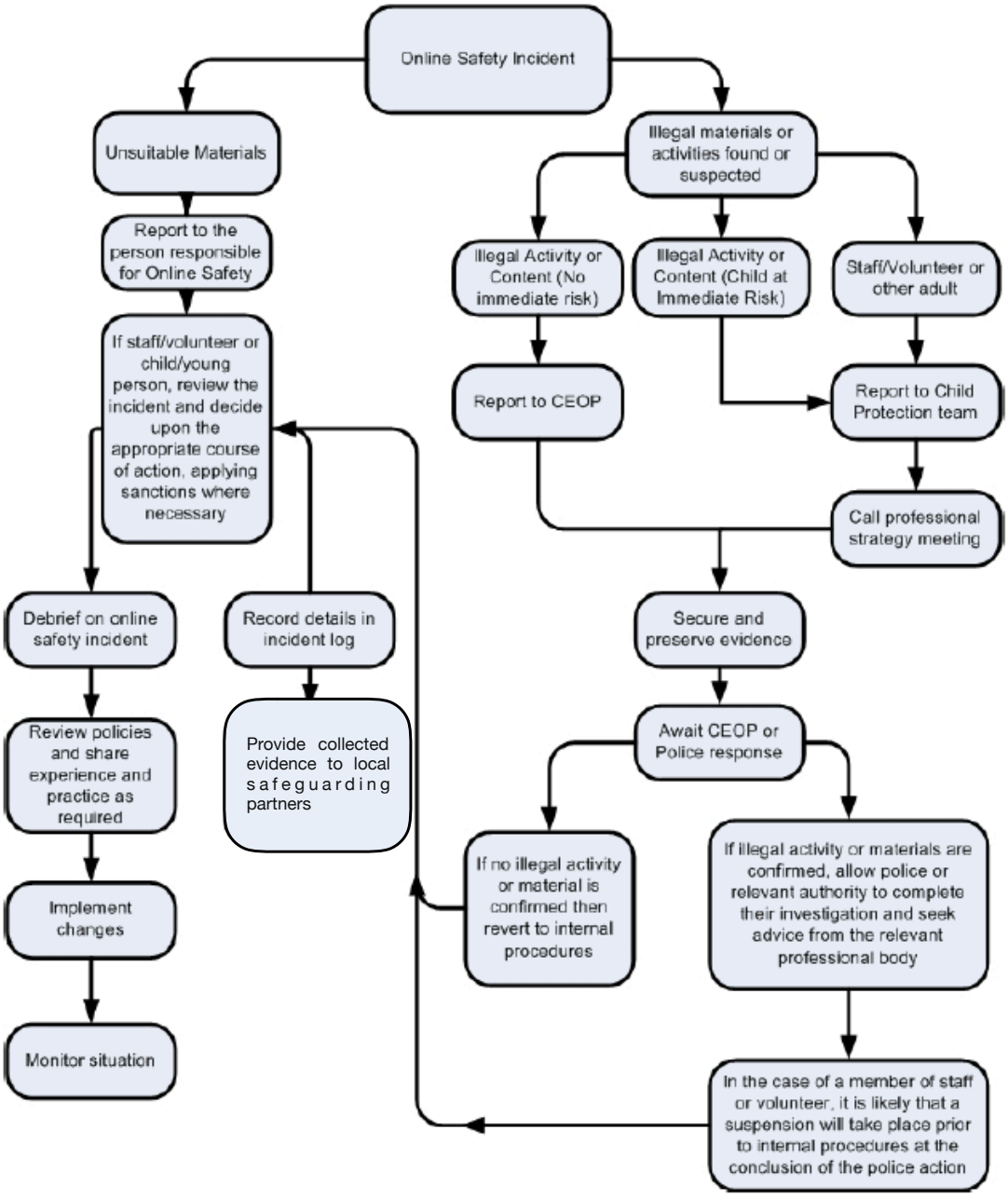
Appendices

1. Responding to incidents of misuse – flowchart

2. Social Media Policy

3. AUP Policies

Responding to incidents of misuse – flow chart



Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

Keble Prep recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by Keble Prep, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.

The school respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with pupilsare also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- SLT
    - Facilitating training and guidance on Social Media use.
    - Developing and implementing the Social Media policy
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
    - Receive completed applications for Social Media accounts
    - Approve account creation
- Administrator / Moderator
    - Create the account following SLT approval
    - Store account details, including passwords securely
    - Be involved in monitoring and contributing to the account
    - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- Staff
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
    - Attending appropriate training
    - Regularly monitoring, updating and managing content he/she has posted via school accounts
    - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook

page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the

matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.

- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- Staff
    - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
    - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
    - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
    - *The school permits reasonable and appropriate access to private social media sites.*
- Pupil/Students
    - Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.
    - The school's education programme should enable the pupils to be safe and responsible users of social media.
    - Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- Parents/Carers
    - If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.

- The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

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

Staff & Volunteer Acceptable Use –

Policy and Agreement

Policy

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. The Internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe Internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Keble Preparatory School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

Keble Preparatory School will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Agreement

- I understand that I must use Keble Preparatory ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
- I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT.
- I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that Keble Preparatory School will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of

school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school.

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. • I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Keble Preparatory School's ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- Any communication with parents will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of Keble Preparatory School:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *Keble Preparatory School* equipment. I will also follow any additional rules set by Keble Preparatory School about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies. (*Now we are on Google this is automatically done online)*

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in Keble Preparatory School policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of Keble Preparatory School:

- I understand that this Acceptable Use Policy applies not only to my work and use of Keble Preparatory School ICT equipment in school, but also applies to my use of Keble Preparatory School ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by Keble Preparatory School.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, suspension, referral to Governors and in the event of illegal activities the involvement of the police.

Please go to the Google form to sign you do not need to sign this document. This is for your reference only.

Pupil Acceptable Use - Policy and Agreement

Year 3– 8 pupils

Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Keble Preparatory school will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

Agreement

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

For my own personal safety:

- I understand that the *Keble Preparatory School* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that Keble Preparatory School systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use Keble Preparatory School systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that Keble Preparatory School has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in Keble Preparatory School I will follow the rules set out in this agreement and Keble's Mobile Device policy, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

When using the Internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the Internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that Keble Preparatory School also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the Form to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign this agreement, access can not be granted to school systems and devices.

Pupil Acceptable Use (Rec- Y2) Policy 2019-20 (Parent copy)

Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Keble Preparatory school will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

Agreement
I understand that I must use Keble Preparatory School ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the *Keble Preparatory School* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that Keble Preparatory School systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use Keble Preparatory School systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that Keble Preparatory School has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in Keble Preparatory School I will follow the rules set out in this agreement and Keble's Mobile Device policy, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

When using the Internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the Internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that Keble Preparatory School also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities the involvement of the police.

Please complete the sections on the attached email form to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.