



Kea C P School

Online Safety Policy

Approved by: Full Governors **Date:** 6 February 2023

Reviewed: Autumn Term 2022

Next review due Autumn Term 2024
by:

Signed by:

Name:

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by the headteacher, ICT4 (the school's ICT support provider) and the full Governing Body. This policy will be reviewed every two years.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity

Scope of the Policy

This Online Safety Policy outlines the commitment of Kea School to safeguard members of our school community online in accordance with statutory guidance and best practice. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Kea 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.

Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges (October 2022) – questions from the Governing Body".

This review will be carried out by the Resources Committee whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Online Safety Lead

- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting to relevant governors group/meeting
- occasional review of the filtering change control logs and the monitoring of filtering logs (where possible)

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Headteacher & Senior Leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.
- 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 staff¹.
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- 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.
- The headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

Online Safety Officer

The headteacher is the Online Safety Officer and will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), where these roles are not combined
 - take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
 - have a leading role in establishing and reviewing the school online safety policies/documents
 - promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
-

- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with local authority, technical staff (ICT4), pastoral staff and support staff (as relevant)
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing body meetings/groups
- report regularly to senior leadership team
- report incidents to the Resources Committee, Senior Leadership Team, ICT4 and ICT Technician.

ICT4 is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection and passwords are regularly changed
- filtering 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 (Online Safety Officer) for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding

- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to the headteacher for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers 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
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the [SWGfL Safe Remote Learning Resource](#)
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Designated Safeguarding Lead

The Designated Safeguarding Lead is trained in Online Safety issues and is aware of the potential for serious child protection/safeguarding issues to arise from:

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

Online Safety

Online safety is included in the role of the safeguarding governor.

Pupils:

Pupils are taught to:

- be responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- understand the importance of reporting abuse, misuse or access to inappropriate materials and how to do so
- know and understand policies on the use of mobile devices and digital cameras, the taking/use of images and on online-bullying.
- 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.

Parents/Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement (the school will need to decide if they wish parents/carers to acknowledge these by signature)
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school
- the use of their children's personal devices in the school (where this is allowed)

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / digital literacy 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 is a focus in all areas of the curriculum and staff 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:

- A planned online safety curriculum is provided as part of ICT/PSHE lessons and is regularly reviewed
- Key online safety messages are reinforced in whole school and class assemblies.
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are 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 are protected and kept safe from terrorist and extremist material on the internet.
- Pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the school.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned pupils are guided to sites checked suitable for their use and there are processes in place for dealing with any unsuitable material that is found in internet searches.
- When pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites visited.
- It is accepted that from time to time, for good educational reasons, pupils 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 ICT4 temporarily remove those sites from the filtered list for the period of study.

Education – Parents/Carers

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.

The school will therefore seek to provide information and awareness to parents and carers through:

- Parent/carers briefing sessions
- Letters, newsletters and the school website
- Parents/Carers evenings/sessions
- Reference to the relevant web sites/publications e.g. [swgfl.org.uk](http://www.swgfl.org.uk)
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

Education & Training – Staff / Volunteers

All staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Staff meetings/INSET days/Child Protection Training.
- All new staff should receive online safety training as part of their induction programme

Training – Governors

Governors are included in any staff online training and it is also included in new governor induction programme. Governors also receive the same online safety information as parents/carers.

Technical – infrastructure / equipment, filtering and monitoring

The school is responsible for ensuring that its infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The headteacher (Online Safety Officer) and Safeguarding Governor are responsible for monitoring the school's infrastructure.

- Regular reviews and audits of the safety and security of school technical systems take place.
- Servers, wireless systems and cabling are securely located with physical access restricted
- All users will have clearly defined access rights to the school's technical systems and devices.
- Only staff are provided with a username and secure password by ICT4 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 regularly.
- ICT4 and the ICT Teaching Assistant 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 the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged

and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

- Internet filtering/monitoring ensures 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.
- School technical staff/ICT4 regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person. Technical incidents are reported to the ICT Technician who then fixes or arranges external support from ICT4 for technical advice. For data breaches the data protection policy is followed.
- The school, through ICT4, uses SENSO cloud alert system to alert the online safety officer of any potential violations of internet use. The online safety officer follows these up and takes action where necessary.
- 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 updated regularly. The school's infrastructure and individual workstations are protected by up to date virus software.
- Any temporary staff or volunteers (e.g trainee teachers, supply teachers etc must read and sign the acceptable use agreement before having access onto school systems.
- The acceptable use agreement details what staff are allowed and forbidden to download and install on school devices.
- The acceptable use agreement details the use of removable media (eg memory sticks / CDs/DVDs) may not be used for any sensitive information (e.g. pupil information) unless encrypted.

Mobile Technologies (including build your own device)

All users understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The acceptable use agreement is consistent with and inter-related with other relevant school safeguarding policies.

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

- Staff are allowed to use school owned devices in school and have full network and internet access. Personal devices are not allowed to be used in school for work purposes. The

use of personal mobile phones is permitted during break times and used in staff areas only and not used in front of pupils (except in an emergency situation e.g. on a school visit).

- Pupils are not allowed to bring personal devices into school. Pupils who need to bring mobile phones to school must hand them in at the school office for safe keeping and collect them at the end of the school day.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils are made 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.

- When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers is obtained before photographs of pupils are published on the school website/social media/local press

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital / video images.

- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; personal equipment of staff should not be used for such purposes.
- Care is 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.

- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school has:

- GDPR Policy.
- Has paid the appropriate fee to the Information Commissioner's Office (ICO).
- Has appointed a Data Protection Officer (DPO) – SchoolPro.
- Will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held is accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- Has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- Clear and understood data retention policies and routines for the deletion and disposal of data.
- Has a procedure for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Considered the protection of personal data when accessing any remote access solutions.
- Has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- Ensures all staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must have approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school practices once it has been transferred or its use is complete.

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

- The official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- All emails from teachers to parents need to go through the school office. School staff are discouraged from being friends with parents on any form of social media.
- Pupils are not provided with e-mail addresses.
- 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

The school has a duty of care to provide a safe learning environment for pupils and staff. It could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party will be dealt with following the school’s disciplinary policy. Reasonable steps to prevent predictable harm are in place.

The school provides the following measures to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Providing training including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Has clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

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

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

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

Personal Use:

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

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the internet for public postings about the school
- The school should respond effectively 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.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. cyber-bullying would be followed up through the school's disciplinary policy. Other activities e.g. accessing child abuse images or distributing racist material is illegal and could also lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

User Actions:

Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

Unacceptable & illegal actions:

- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008
- 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

Unacceptable actions:

- Pornography
- Promotion of any kind of discrimination
- Threatening behaviour, including promotion of physical violence or mental harm
- Promotion of extremism or terrorism

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

Acceptable at certain times but only for school purposes e.g. Amazon purchases or school social media account:

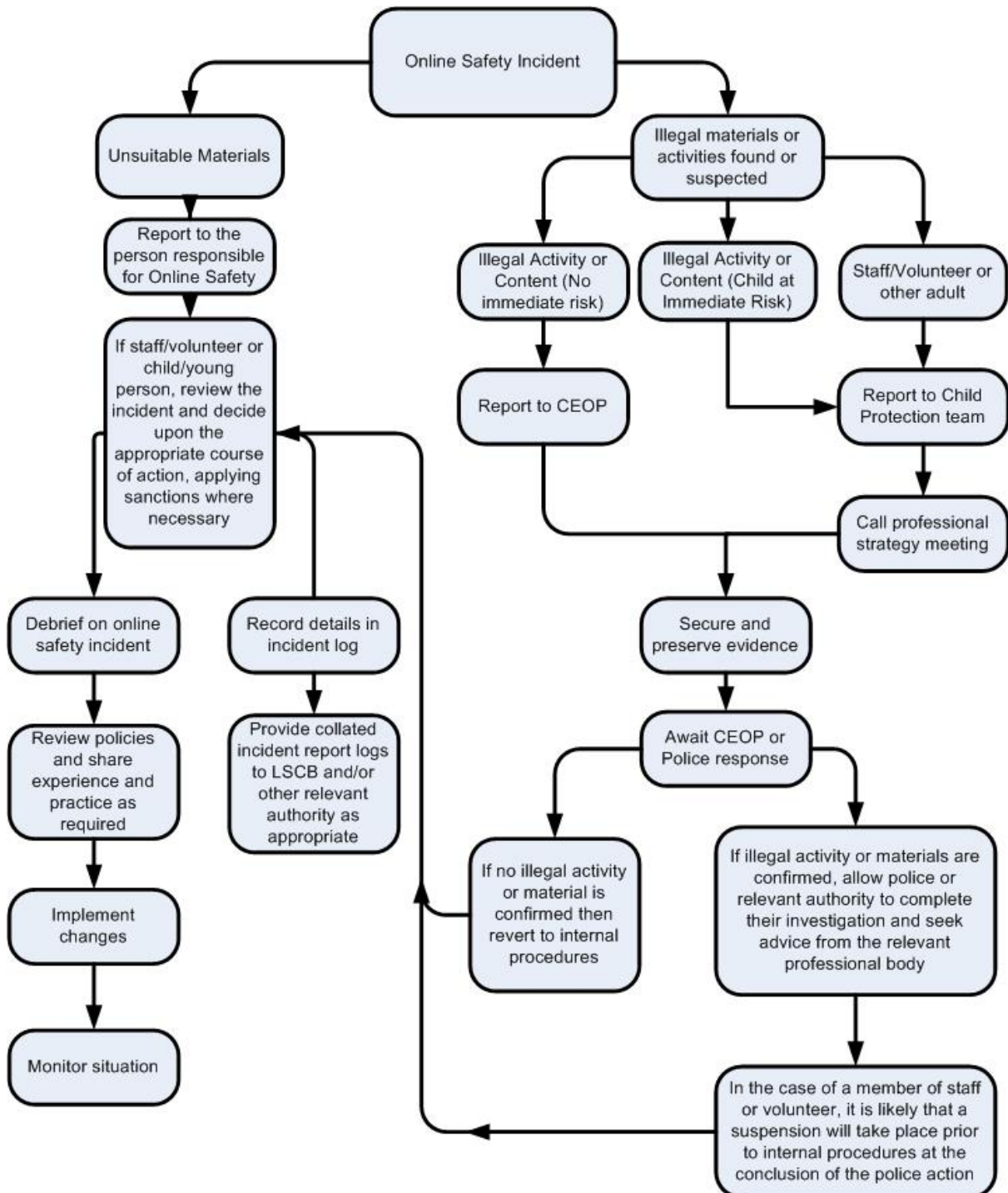
- On-line shopping/commerce
- File sharing
- Use of social media
- Use of messaging apps
- Use of video broadcasting e.g. Youtube

Responding to incidents of misuse

The guidance below is for staff use to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident.

Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority
 - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for

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

School 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 as follows:

Pupils Incidents	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access	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			X		X	
Unauthorised / inappropriate use of mobile phone / digital camera / another mobile device		X			X		X	
Unauthorised / inappropriate use of social media / messaging apps / personal email		X			X		X	
Unauthorised downloading or uploading of files		X			X		X	
Allowing others to access school / academy network by sharing username and passwords		X			X		x	

Attempting to access or accessing the school network, using another pupil's account		X			X	X		
Attempting to access or accessing the school network, using the account of a member of staff		X			X	X		
Corrupting or destroying the data of other users		X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X	X		
Continued infringements of the above, following previous warnings or sanctions		X			X	X	X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X	X		
Using proxy sites or other means to subvert the school's filtering system		X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X			
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X		X	X		

Actions / Sanctions

Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to Local Authority /	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Potential Disciplinary action	Refer to GDPR
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			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
Deliberate actions to breach data protection or network security rules		X	X					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	
Actions which could compromise the staff member's professional standing		X						X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X						X	
Using proxy sites or other means to subvert the school's filtering system		X	X	X				X	

Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X				X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X				X
Breaching copyright or licensing regulations		X	X					X
Continued infringements of the above, following previous warnings or sanctions		X						X

Appendix

Pupil Acceptable Use Agreement



School 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 Agreement 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 will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my own personal safety:

- I understand that the 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 (At Kea pupils do not communicate with others online in school, but they are taught how to keep themselves self when using ICT in their own time).
- 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)
- 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 the 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 the 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 towards 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 the 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 not use my own personal devices (mobile phones/USB devices etc) in school.

- 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 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 not access social media sites.

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 the 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 sanctions. 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 next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Policy Agreement



This is how we stay safe when we use computers:

- I will ask a member of staff if I want to use the computers / iPad.
- I will only use activities that a member of staff has told or allowed me to use.
- I will take care of all ICT equipment.
- I will ask for help from a member of staff if I am not sure what to do or if I think I have done something wrong.
- I will tell a member of staff if I see something that worries or upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer / iPad

Signed (parent): _____

Pupil's Name _____

Year Group: _____

Date: _____