Online Safety Policy

Policy review dates and changes

Review Date	By Whom	Summary of Changes	Date implemented
May 2018	J.Flint	Updated in line with latest DfE guidance/expectations, CEOP and SWGfL	June 2018
May 2019	J.Flint	Updated key individuals.	June 2019
February 2020	J.Flint	Updated key individuals.	September 2020
November 2020	J.Flint	Added remote learning, added references to Staff Code of Conduct, updated AUAs	December 2020
January 2021	J.Flint	Added loaning of ICT equipment into remote learning section, added Appendix 3	January 2021

Introduction

This document outlines Griffe Field Primary School's Online Safety Policy. It applies to all adults, including volunteers working in or on behalf of the school, pupils and members of our wider school community. This policy works in conjunction with the schools policy on 'Child Protection and Safeguarding' but has a greater focus on specific issues relating to technology, communication and the internet.

Aims of the Policy

The aim of this policy is to ensure that all members of our school community are guarded against the potential issues inherent from using the internet and different technologies. The safety and wellbeing of pupils and staff is one of the highest priorities we hold, and for more information on how we do this, please refer to the 'Child Protection and Safeguarding Policy'

Purposes of the Policy

The central purpose of this policy is to ensure all members of the school community are aware of their responsibilities in relation to online safety. It also highlights the key issues relating to online safety and the procedures that need to be undertaken if there is a safety issue.

Development, Monitoring and Review

This Online Safety policy has been developed by the Computing Coordinator, in conjunction with the Headteacher and Senior Leadership Team.

This policy will be reviewed annually.

Key Individuals

Throughout this policy, a number of individuals are cited with their roles and responsibilities. These individuals are identified below.

Headteacher (also Designated Safeguarding Lead (DSL))	Emma Mitchell
Deputy DSL	Lucy Morton
Other Members of the Senior Leadership Team	Ravi Dulai (Deputy Head) Donna Webb Hayley Dean Jack Flint
Computing Coordinator(s)	Sadie Coles Jack Flint
Chair of Governors	Chrissy Diffin, John Reaveley
Governor responsible for Child Protection and Safeguarding	Helen Hicks
Technical Support Staff	Provided by Mercury AVS Ltd.

Roles and Responsibilities

The Headteacher and the Senior Leadership Team

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will monitored by the Computing Co-ordinator. If any incidents are believed to be a safeguarding issue, then this is to be immediately referred to the Designated Safeguarding Lead and/or Deputy DSL.

The Headteacher and the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety incident. These include following safeguarding procedures (outlined in the Child Protection and Safeguarding Policy).

The Headteacher and Senior Leaders are responsible for ensuring that all relevant staff receives suitable training to enable them to understand and deal appropriately with issues relating to online safety.

The Senior Leadership Team 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 to give support to colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the Computing Co-ordinator regarding any arising issues as a result of using new technologies, arising issues (local or national) and from recent training.

Computing Coordinator

In addition to their role in leading and monitoring the teaching and learning of computing (see Computing Teaching and Learning Policy), the Computing Coordinator:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies
- 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 the Designated Safeguarding Lead to stay up to date with local/national issues relating to online safety
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, (Examples of suitable log sheets may be found later in this policy)

School Staff

All staff working in school are to adhere to the policies and procedures outlined to safeguard children and adults in school. This includes monitoring and reporting any issues where a member of our school community is at risk.

In terms of Online Safety, School staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement (AUA). This can be found in Appendix One.
- they report any suspected misuse or problem to the Headteacher (DSL), Senior Leader or Computing Coordinator for investigation / action / sanction
- all digital communications with pupils / 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
- pupils understand and follow the Online Safety Policy and acceptable use policies
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, 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

Governing Body

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing body, receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Child Protection and Safeguarding. This specific role is highlighted in the Child Protection Policy and Safeguarding and include the monitoring, discussing and reporting of any online safety incidents.

Technical Support Staff

The Computing Technicians are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy or Guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection system, in which passwords are regularly changed
- the school internet access is filtered, and that it is 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 and email system is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher (DSL), Senior Leaders or Computing Co-ordinator for investigation / action / sanction
- that monitoring software and systems are implemented and updated as agreed in school policies

Pupils

All pupils in school:

- are responsible for using the school digital technology systems in accordance with the Pupil AUA, found in Appendix Two
- 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 the school's / Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents and the Wider Community

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet, technology and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, Remote Learning Platform and information about national / local online safety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to the website and Learning Platform and on-line pupil records
- that children's personal devices are not to be brought into school without express permission

Other adults in school, including students on placement, volunteers PTA helpers and other community users who access school systems as part of the wider school provision will be expected to read, understand and sign the Staff AUA (appendix one) before being provided with access to school systems.

Policy Statements

Acceptable Usage Agreements (AUA)

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 new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should always have an entitlement to safe internet access.

The Acceptable Usage Agreements (AUA) are outlined in the appendices. These agreements are 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.
- that adults working in school are responsible for their use of both school owned and personal technologies. This includes responsible use of devices and being vigilant to issues relating to safeguarding, data protection and professionalism.
- that students, volunteers and community users are aware of the need for safe and responsible use of technology whilst in school.

Appendix One shows the AUA for staff members, students and volunteers.

Appendix Two shows the AUA for pupils.

Education of Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages 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 should be provided as part of the Computing and PHSE subject areas. It should also be covered in other subject areas where applicable, and regularly revisited throughout the year.
- Key online safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. (for more information on PREVENT duties, see the Child Protection and Safeguarding Policy).
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education of Parents, Carers and the Community

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 and 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:

- Curriculum activities
- Letters, newsletters, website, Remote Learning Platform
- Parents Evenings
- Parent Workshops
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant websites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

The school will provide opportunities for local community members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community

Education and Training of Staff, Volunteers and Governors

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.*
- *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.*
- *It is expected that some staff will identify online safety as a training need within the performance management process.*
- *The Computing Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The Online Safety Coordinator will provide advice, guidance and training to individuals as required.*

Governors should take part in online safety training and awareness sessions, with particular importance for those who are members with responsibilities for child protection, safeguarding or part of any subcommittee involved in technology or the teaching and learning of computing and online safety. This may be offered in a number of ways:

- *Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).*
- *Participation in school training and/or information sessions for staff or parents (this may include attendance at assemblies / lessons).*

Technical Security, Filtering and Monitoring

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

- *School technical systems will be managed in ways that ensure that the school meets recommended technical requirements*
- *There will be regular reviews and audits of the safety and security of school technical systems*
- *Servers, wireless systems and cabling must be securely located and physical access restricted*
- *All users will have clearly defined access rights to school technical systems and devices.*
- *All pupil users from Year Two up to Year Six are provided with a username and secure password to access the school laptops and network. Year One and*

Foundation Stage users are to use a shared user and password. Staff users are all provided with unique usernames and passwords. A record of these are to be kept by the technical staff.

- The "administrator" passwords for the school ICT system, used by the technical support staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- The technical support staff is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (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 (see above in 'Education of Pupils' policy statement.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet
- The school has provided differentiated user-level filtering, allowing staff to access additional websites necessary for their role that are deemed inappropriate for children to use (such as Youtube)
- School technical staff 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.
- 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. The school infrastructure and individual workstations are protected by up to date virus software.

Mobile Technologies

Mobile technology devices may be provided or owned by the school 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 devices in a school context is educational. Personal devices, owned by staff or children, are not to be used in school to support teaching and learning.

More information relating to personal devices is outlined in the Acceptable Usage Agreements, outlined above and in the appendices.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

For more information, please refer to the Data Protection Policy.

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 (many memory sticks / cards and other mobile devices cannot be password protected)
    - the device must offer approved virus and malware checking software
    - the data must be securely deleted from the device once it has been transferred or its use is complete

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place.

Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, Learning Platform or local press
- Parents and carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). These images should only include their own child(ren) unless they have sought permission from other parents/carers to include them too. To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents or carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school /equipment, the personal equipment of staff should not be used for such purposes.
- Volunteers, including student teachers, teaching assistants or other students undergoing training or work experience must gain permission from a member of the Senior Leadership Team before taking any photographs or videos in school. Any digital images or videos of the pupils must not include faces or names where individuals can be identified.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. These include the use of mobile devices, email services, blogging, instant messaging, communicating through the Learning Platform and social media.

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report to the DSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- *Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, Learning Platform etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class email addresses may be used at KS1, while pupils at KS2 and above 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.*

Remote Learning

In light of Coronavirus pandemic, schools have had to respond quickly and proactively providing remote learning using various means. Please refer to Griffe Field's policy on remote learning for more details.

Ensuring safety online when delivering and participating in remote learning provides its own challenges, which all participants must consider.

At all times, participants must abide by their relevant 'AUA' when participating in remote learning.

Under some circumstances, pupils/families may require the loan ICT equipment (such as laptop, tablets etc) from school. Some of these are school resources, other provided by the government. These resources are loaned under the agreement outlined in appendix three and with the consent of the school.

Pupils Remote Learning

Extra emphasis is placed on parents and carers to be responsible for ensuring that children's online safety is assured if they are required to take part in remote learning.

School staff must also take into account their role in making sure that what is set is in the best interest in the children's safety online as well as their education.

The following considerations must be made in order to facilitate remote learning for pupils.

- Pupils must only use their Remote Learning Environment (Microsoft Teams) for the purpose of school work and collaboration. It is not for personal use.
- Staff must use their work account to manage remote learning and not a personal account.
- Other parties, including parents are expected to give appropriate support for children to access their home learning.
- Pupils must use their own log in details to access the remote learning, and not that of another child.
- Parents/carers must support and monitor their children's use of the remote learning platform to ensure that it is used appropriately and that they adhere to the AUA.
- If pupils are to submit any work, including multimedia such as photographs or videos, they must be vigilant not to share anything that might be seen by their peers or other parties that may leave them vulnerable to harm, including bullying, cyberbullying, abuse or any other issue outlined in the safeguarding policy.
- When setting work, school staff need to consider what work is appropriate to be completed outside of a classroom environment. This is to prevent children being at risk to viewing inappropriate content or any other online safety issue.
- School Staff and the Technical Support staff must monitor how the Remote Learning Platform and pupils emails are used to avoid misuse. Any inappropriate actions made must be handled appropriately using guidance later in this policy and by following normal safeguarding procedures.

- Pupils must not change their passwords to access remote learning without express instruction from school staff.
- School staff must keep record of pupils log in information to ensure effective monitoring can be carried out.

Staff Networking, CPD and Training

Since the Coronavirus lockdown, many CPD, staff training and networking events have taken place remotely via the internet. When taking part in any online networking, school staff must take the following measures to ensure the online safety of themselves and others.

- Staff must adhere to the Staff Code of Conduct Policy when remote networking.
- Staff must use their work account for Zoom/Microsoft Teams when taking part in online networking or training.
- School equipment must only be used for school remote networking and not for personal remote networking.
- Staff must be mindful of where they take part in the remote networking. Remote networking must take place in an appropriate space, either on the school site or in a private residence. Public places are not appropriate. This also includes using a public internet connections, such as free wifi.
- If sharing a video using a webcam, staff must consider their immediate environment to ensure the safety of themselves and others. This could include personal photographs if at home or displays showing pupils names or pictures in school.

Social Networking and Social Media

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

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

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

School staff should ensure that:

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

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 effectively respond to social media comments made by others according to a defined policy or process.

Unsuitable and Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems.

Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

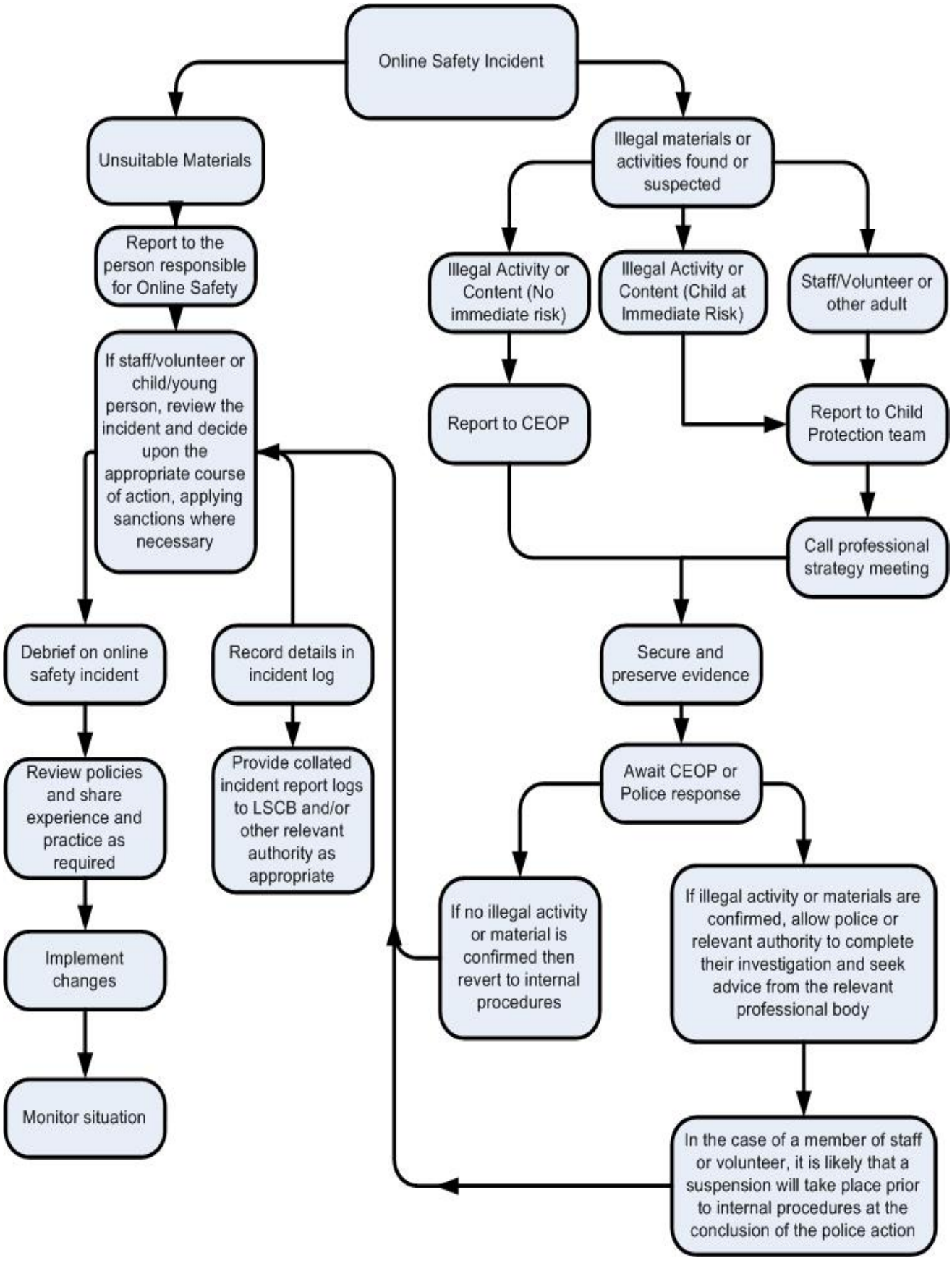
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities, as listed above.

If there is a suspicion of an illegal activity, please refer to the right side of the flowchart overleaf.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Actions/Sanctions

Any issues involving online safety and/or the misuse of ICT resources will be dealt with on a case by case basis.

For pupils, the severity of the incident will be assessed by the class teacher. The schools rewards and sanctions procedures will be followed and the case escalated to the safeguarding team if required (in accordance with the schools positive behaviour and safeguarding policy)

For incidents involving staff, procedures such as staff disciplinary procedures, safeguarding and whistleblowing must be followed.

Appendices

Appendix One – Acceptable Usage Agreement – Staff, Students and Volunteers

School Staff Acceptable Use 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. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. 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 digital technology 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 school / academy 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. I will not use my personal equipment (including tablets, cameras and phones) to record these images, unless I have permission to do so. 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 social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal devices (laptops / tablets / 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 school equipment. I will also follow any additional rules set by the 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 use personal email addresses on the school ICT systems.
- 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.
- 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 school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local

network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

- 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 the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the 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, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....
Signed: .....
Date: .....

School Acceptable Use Agreement

- I will not share my personal information with others online.
- I will not ask others to share their personal information with me online.
- I will ask an adult if I want to use the computers / tablets
- I will only use activities that an adult has told or allowed me to use
- I will be responsible and make good choices whilst using electronic devices, computers and the internet.
- I will take care of the computers and other equipment
- I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher if I see something that upsets me on the screen
- I will only use my own user name and password and I will keep my password safe
- I will think SMART!
- I know that if I break the rules I might not be allowed to use the school's technology.

Appendix Three - Agreement for Loaning School ICT Equipment to Parents/Families

Agreement for Loaning School ICT Equipment to Parents/Families

This agreement is between Griffe Field Primary School and parents whose children are borrowing school ICT equipment. This agreement has been agreed by the school's Senior Leadership Team is valid from XXth January 2021. This agreement has been created to ensure you understand your responsibilities as a parent whilst your child is borrowing ICT equipment from the school.

Device(s) Name / Description : .....

Device(s) Serial Number : .....

The device(s) listed above are the property of the school and activity can be monitored for any breaches of the school's 'Acceptable Use Agreement' outlined in the Online Safety policy.

Please read the statements below and tick to say that you understand and agree to the terms, then sign at the bottom.

Responsibilities

- You must ensure that nobody other than your child has access to the device.
- You must ensure that the device is used for the sole purpose of supporting your child's education.
- You must ensure that the device is not used for any personal uses, by your child or anyone else.
- You must ensure that the device is stored safely.
- You must ensure that the device is not used near any food or drink.
- You must ensure that your child understands how to use the device properly, safely and in line with the school agreement.
- If the device is damaged, you must report it to school immediately.
- If the device is lost or stolen, you must report it to school and the police immediately.
- If the device is damaged in any way whilst in your child's possession, you must pay for the replacement or repair costs.
- If any covers, chargers or other equipment loaned with the device are damaged whilst in your child's possession, you must pay for the replacement or repair costs.
- If there is any software issues or damage (e.g. viruses, connectivity issues etc) you must report this to school immediately.
- You must not remove any apps or programs or install any new apps or programs to the device. If there is software that is a necessity but not installed on the device, inform the school immediately so this can be reviewed.
- You must ensure that no applications are disabled on the device, modify the device in any way or sync the device up with any personal devices or equipment at home.

Please tick and sign below.

- □ I will carry out my responsibilities as outlined in this agreement.
- □ I understand that I must pay for any loss or damage to the device(s) and/or the associated equipment named on this agreement.

Parent Name (please print) : .....

Parent Signature : ..... Date : .....

Staff Member loaning the device(s) (name and sign) : .....