Sleights Church of England
(Voluntary Controlled) Primary School

Online Safety Policy

September 2018

Scope of the Policy
This policy applies to all members of the Sleights Church of England (VC) Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of Sleights Church of England (VC) Primary School digital technology systems, both in and out of school.

Sleights Church of England (VC) Primary School will deal with 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
The following section outlines the online safety roles and responsibilities of individuals and groups within the Sleights Church of England (VC) Primary School:

Governors
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor / Director. This is Gemma Kellerman.

Headteacher
The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community. The Headteacher will follow procedures in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents).

The Headteacher is responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Network Manager (Schools ICT) will be responsible for:
- that the school's / academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the Sleights Church of England (VC) Primary School meets required online safety technical requirements and any Local Authority other relevant body Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), 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 / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in Sleights Church of England (VC) Primary School policies

Teaching and Support Staff
Are responsible for ensuring that:
- they have an up to date awareness of online safety matters and of the current Sleights Church of England (VC) Primary School Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)

- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- all digital communications with students / 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
- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, 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 students / 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

Designated Safeguarding Lead

- Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Students:

- are responsible for using the Sleights Church of England (VC) Primary School digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on 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 / academy's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The Sleights Church of England (VC) Primary School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the Sleights Church of England (VC) Primary School in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line student / pupil records

Policy Statements

Education – Students / Pupils

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 Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / 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. Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside Sleights Church of England (VC) Primary 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 students / 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 students / 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 – 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.

Sleights Church of England (VC) Primary School will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix for further links / resources)

Education & Training – Staff / Volunteers

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:

- Online safety training
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the Sleights Church of England (VC) Primary School Online Safety Policy and Acceptable Use Agreements.

Technical – infrastructure / equipment, filtering and monitoring

The Sleights Church of England (VC) Primary School will be responsible for ensuring that the Sleights Church of England (VC) Primary 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:

- Sleights Church of England (VC) Primary School technical systems will be managed in ways that ensure that the Sleights Church of England (VC) Primary School meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of Sleights Church of England (VC) Primary 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 Sleights Church of England (VC) Primary School technical systems and devices.
- All users will be provided with a username and secure password
- Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the Sleights Church of England (VC) Primary School ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher.

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.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Sleights Church of England (VC) Primary School has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.)
- Sleights Church of England (VC) Primary 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.
- An appropriate system is in place (to be described) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place (schools / academies may wish to provide more detail) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / 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 students / 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 students / 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 Sleights Church of England (VC) Primary School events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow Sleights Church of England (VC) Primary School policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Sleights Church of England (VC) Primary School equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Sleights Church of England (VC) Primary School into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

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. (many memory sticks / cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software.

- The data must be securely deleted from the device, in line with Sleights Church of England (VC) Primary School policy once it has been transferred or its use is complete.

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

- The official Sleights School email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- 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.
- Students / 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 / academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

School staff should ensure that:

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

When official school / academy 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 / academy disciplinary procedures

Summary of Technology use in school

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how many schools currently consider the benefit of using these technologies for education purposes against the risks and disadvantages. This is for guidance only and your school will need to decide on what is right for your school

	Staff and other adults					Pupils				
Communication Technologies	Permitted	Permitted	Permitted at certain times	Permitted for named staff	Not Permitted	Permitted	Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones	✓									✓
Mobile phones used in lessons					✓					✓
Use of mobile phones in social time	✓	Where no children are present								✓
Staff should only contact a pupil on the school telephone	✓									
Taking photographs/film on personal mobile devices / digital camera					✓					✓
Taking photographs/film on school mobile devices / digital camera for school purposes only	✓								✓	
Parent / carer taking photos of a school event on their own device and uploading online with public access					✓					✓
Use of personal tablets/ laptops					✓					✓

ipads etc in school							
Use of school owned tablets/ laptops/ ipads in school but not for personal use		✓			✓		
Use of school owned tablets/ laptops/ ipads out of school but not for personal use		✓ (within the AUP)			✓ (within the AUP)		
Only using school provided encrypted storage devices		✓			✓		
Use of school email for personal emails			✓				✓

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

- The official school email service may be regarded as safe and secure and is monitored. Staff, governors, volunteers and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person (in accordance with the school policy) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, governors and pupils or parents/carers (email, chat, 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 public chat/social networking programmes must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff and governors.

Summary of Unsuitable / inappropriate activities

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Any Hate Crime – motivated by hostility on the grounds of race, religion, sexual orientation, disability or transgender identity.					✓
Promotion of any kind of extremist activity					✓
Promotion of racial or religious hatred					✓
Accessing any extremist materials online (e.g Far Right Extremism)				✓	
Threatening behaviour, including promotion of physical violence or mental harm					✓
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute e.g discussing school issues on social media				✓	
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✓	

Creating or propagating computer viruses or other harmful files				✓
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓
On-line gaming (educational)		✓		
On-line gaming (non- educational)				✓
On-line gambling				✓
On-line shopping / commerce			✓	
File sharing			✓	
Use of social networking sites			✓	
Downloading video broadcasting e.g. Youtube for educational purposes	✓			
Uploading to video broadcast e.g. Youtube			✓	