St Nicholas' CE (VA) Primary School

Online Safety Policy

November 2022-November 2023

SWGfL
Safe, Secure, Online

Contents:

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Full Governing Body on:	November 2022
The implementation of this online safety policy will be monitored by the:	SLT
Monitoring will take place at regular intervals:	Termly
The Governing Body will receive a report on the implementation of the online safety policy (which will include anonymous details of online safety incidents) at regular intervals:	Once a Year – July 2023
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Annually – November 2023
Should serious online safety incidents take place, the following external persons/agencies should be informed as appropriate	LA Safeguarding Officer, LADO, Police

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
- Surveys/questionnaires of
    - students/pupils
    - parents/carers
    - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour as per School Behaviour Policy. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines 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. 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*. The role of the Online Safety *Governor* will include:

- regular meetings with HT/DHT or Oakford
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors Committee meeting

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community. The day to day responsibility for online safety is delegated to Oakford Technology.
- The Headteacher is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant LA procedures).
- The Senior Leadership Team will receive regular monitoring reports from Oakford from their quarterly consultation meetings.

Online Safety Lead

The Headteacher and Oakford will work together within the Online Safety Group to:

- take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority
- liaise with school technical staff
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments,
- meet regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs

Technical staff

Those with technical responsibilities through Oakford 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/MAT/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
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy Template" for good practice)
- 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 networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders) for investigation.
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices annually.
- they have read, understood and signed the staff acceptable use policy (AUP) Appendix B
- they report any suspected misuse or problem to the Headteacher for investigation
- 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 Appendix B
- 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 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/DDSL

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

Online Safety Group

The Online Safety Group (Online Safety Governors, Headteachers and Oakford technology) will ensure:

- the monitoring of the school online safety policy.
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the pupils about the online safety provision
- monitoring improvement actions identified

Pupils:

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement (Appendix C)
- 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 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 school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, website 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 (Appendix D)
- access to parents' sections of the website/Learning Platform and on-line pupil records

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. 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 lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and whole class activities
- 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.
- 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. (Covered through SMSC, RE, PSHE Policy and RE and PSHE scheme of work)
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement (Appendix c) and encouraged to adopt safe and responsible use both within and outside school.
- 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 (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that Oakford can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be recorded on the Temporary Filter Removal Log (Appendix H), 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.

The 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 F 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:

- A planned programme of formal online safety training will be made available to staff and logged on the school's Single Central Record (SCR). 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 possible that some staff will identify online safety as a training need within the performance management process.
- The Headteacher will receive regular updates through attendance at external training events 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 training sessions. The staff will sign a register to confirm that they have read, understood and agreed the policy.
- The Headteacher will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

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

Technical – infrastructure/equipment, filtering and monitoring

The Online Safety Group 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 periodic reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users have access to a class login and password within school

- All children have a password and login to access Google Classrooms/Professor Assessor/Numbots and are taught about the importance of keeping logins safe and private
- The "master/administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- Oakford 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider (delegated to Oakford). 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 should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Oakford 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 (see Policy Appendix B).
- Users/staff should report any actual/potential technical incident/security breach to the Headteacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- A Staff (and volunteer) Acceptable Use Policy and Agreement is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school. This is read, understood, agreed and copied for all staff and a master copy kept and retained by the School (see Policy Appendix B).
- A Staff (and volunteer) Acceptable Use Policy and Agreement is in place that forbids staff from downloading executable files and installing programmes on school devices. This is read, understood, agreed and copied for all staff and a master copy kept and retained by the School (see Policy Appendix B).
- It is agreed that staff will not use removable devices to store sensitive information (e.g. memory sticks/CDs/DVDs) by users on school devices. All devices have been disabled other than the Headteacher and Admin Officer. School confidential information, records etc. cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Internal communications are exempt.

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 online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. 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/social media/local press (Appendix D)
- 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 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 pupils in the digital/video images. (Appendix D)

- 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.(Appendix B)
- 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.
- 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.
- 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/academy must ensure that:

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only 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. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it provides staff, parents and volunteers with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners

- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device eg laptop the:

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

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
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices ie laptops these must be encrypted and password protected.
- will not transfer any school personal data to personal devices or removable devices e.g USBs except as in line with school policy
- access personal data sources and records 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

Communications

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

Communication Technologies	Staff & other adults				Students/Pupils				
	Allowed	Allowed at certain times	Allowed for selected staff	Not Allowed	Not allowed	Allowed	Allowed at certain times	Exceptional Circumstances with HT Permisssion	Not allowed
Mobile phones may be brought to the school/academy	X							X	
Use of mobile phones in lessons					X				
Use of mobile phones in social time		X			X				
Taking photos on mobile phones/cameras				X	X				
Use of other mobile devices e.g. tablets, gaming devices	X						X		
Use of personal email addresses in school, or on school network		X			X				
Use of school email for personal emails				X	X				
Use of messaging apps on personal devices		X							
Use of Personal Social Media (see Policy on Personal use of social media by teaching and support staff in school)		X							
Use of School Social Media			X						
Use of blogs			X						

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.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school/academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- All children will be provided with their own email address via Google Classrooms for educational use only
- 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.

- Pupils needing to bring a mobile device to school under exceptional circumstances must seek written permission from the Headteacher.

Social Media - Protecting Professional Identity

All schools 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, engage in online bullying, 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

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
- Members of staff should not be 'friends' with parents of the school on social media unless exceptional circumstances agreed by the Headteacher.

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

Dealing with unsuitable/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/academy when using school/academy 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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools/academies will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to						X

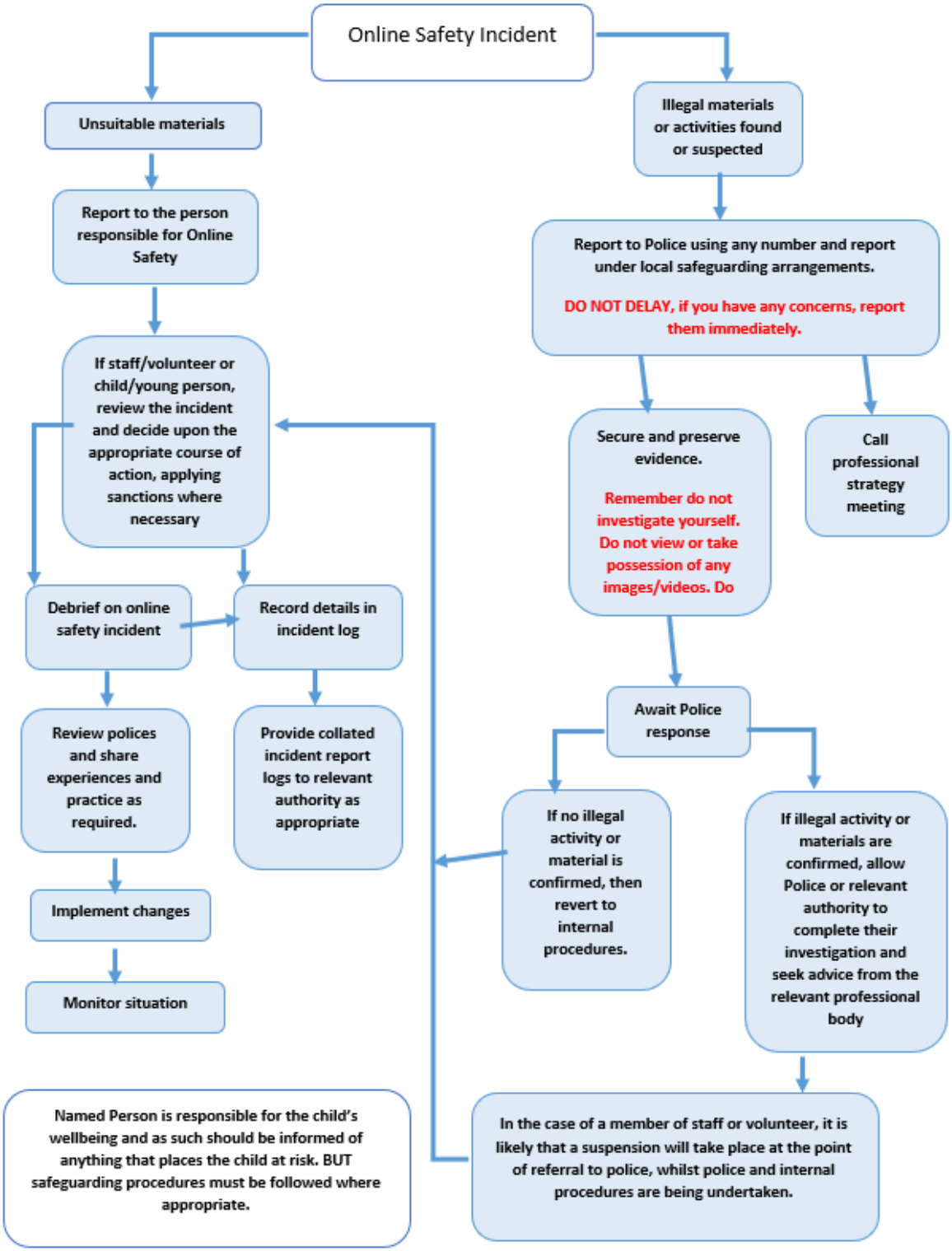
prevent young people becoming involved in cyber-crime and harness their activity in positive ways.					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				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 (see "User Actions" above).

Illegal Incidents

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



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.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- 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 Reporting Log 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/Academy Group or national/local organisation (as relevant).
    - 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
    - offences under the Computer Misuse Act (see User Actions chart above)
    - 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:

Students/Pupils Incidents	Refer to class teacher/tutor	Refer to Headteacher/Deputy Head	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. 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					
Unauthorised use of non-educational sites during lessons	X			X			X	
Unauthorised/inappropriate use of mobile phone/digital camera/other 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			X	
Allowing others to access school network by sharing username and passwords	X				X		X	
Attempting to access or accessing the school network, using another pupil's account	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			X			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		
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			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		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X			X		X	

Staff Incidents	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Management guidance	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X				X
Inappropriate personal use of the internet/social media/personal email				X		
Unauthorised downloading or uploading of files			X	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		
Careless use of personal data e.g. holding or transferring data in an insecure manner				X		X
Deliberate actions to breach data protection or network security rules					X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software				X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature				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	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
Breaching copyright or licensing regulations		X		X		
Continued infringements of the above, following previous warnings or sanctions	X			X	X	X

School Technical Security (including filtering and passwords)

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of Oakford with the Headteacher.

Technical Security

The school will be responsible for ensuring that their 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 receive guidance and training and will be effective in carrying out their 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
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school/academy systems and data
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff at Oakford
- all users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded Oakford and will be reviewed, at least annually, by the online safety group.
- users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- Oakford 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
- Oakford 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 to the online safety group ie. pupils will report to class teachers and class teachers will report to HT/Oakford.
- an agreed policy is in place (to be described) for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school/academy system
- an agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users
- an agreed policy is in place regarding the extent of personal use that users (staff/children) and their family members are allowed on school devices that may be used out of school
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school/academy devices. Removable media should not be used to store data about pupils.

- the school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- personal data cannot be sent over the internet or taken off the school/academy site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform).

Policy Statements:

- These statements apply to all users.
- All school networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group (or other group).
- All users (adults and pupils) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All pupils will be provided with a username and password for google classroom which will be stored securely on staff share so that teachers have access.
- All teachers will generate their own passwords which will be updated as required. Logins will be given to Lisa Glover and stored securely.

Password requirements:

- Passwords should be at least 8 characters long. Passwords should be easy to remember, but difficult to guess or crack.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school/academy
- Passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system

Learner passwords:

- Records of learner usernames and passwords for pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- Students/pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.
- All pupils in each class have a class username and password to access computers in school but an individual log in for online learning platforms e.g. Professor Assessor, Numbots and Google Classrooms.

Notes for technical staff/teams

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration should also be given to using two factor authentication for such accounts.
- An administrator account password for the school systems should also be kept in a secure place e.g. school safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.
- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.

- It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.
- Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by SLT/Office
- Good practice is that the password generated by this change process should be system generated and only known to the user. This password should be temporary and the user should be forced to change their password on first login. The generated passwords should also be long and random.
- Where automatically generated passwords are not possible, then a good password generator should be used by SLT/Office) to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login.
- Requests for password changes should be authenticated SLT/Office to ensure that the new password can only be passed to the genuine user .
- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use.
- In good practice, the account is "locked out" following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).

Training/Awareness:

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the acceptable use agreement

Students/pupils will be made aware of the school's/college's password policy:

- in lessons through safety lessons and reinforcement throughout the year.
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:

The Online Safety Group will ensure that full records are kept of:

- User Ids and requests for password changes
- User logons
- Security incidents related to this policy

Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school. The school can act with flexibility to allow access to sites which would otherwise be filtered to enhance children's education within appropriate age groups.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by Oakford. They will manage the school filtering, in line with this policy and along with the Online safety group will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to the Headteacher prior to changes being made

All users have a responsibility to report immediately to Headteacher any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- *The school maintains and supports the managed filtering service provided by the Internet Service Provider*
- *The school has provided enhanced/differentiated user-level filtering through the use of the* Oakford *filtering programme. (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc.)*
- *Any filtering issues should be reported immediately to the filtering provider.*
- *Requests from staff for sites to be removed from the filtered list will be considered by Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.*

Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the acceptable use agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the acceptable use agreement.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school online safety policy and the acceptable use agreement. *Monitoring will take place by Oakford and they will report regularly to the Online Safety Group within school.*

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- Online Safety Group
- Online Safety Governor
- External Filtering provider/Local Authority/Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Further Guidance

Schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, 2015).

The Department for Education 'Keeping Children Safe in Education' requires schools to: *"ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system"* however, schools will need to *"be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."*

In response UKSIC produced guidance on – information on "Appropriate Filtering"

Somerset Guidance for schools – questions for technical support – this checklist is particularly useful where a school/academy uses external providers for its technical support/security.

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed: SWGfL Test Filtering

Electronic Devices - Searching & Deletion

The changing face of information technologies and ever increasing pupil/student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Head Teacher must publicise the school behaviour policy, in writing, to staff, parents/carers and pupils at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies" (2014 and updated January 2018)

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

Responsibilities

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will be taken to Governors for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: Headteacher/Deputy Head

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data/files on those devices: Lucy Hill (Deputy Head) Leanne Smith (SENCO)

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Training/Awareness

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data/files on those devices.

Pupils are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school.

If pupils/students breach these roles:

The sanctions for breaking these rules will be proportionate to the situation e.g accidental or brought into school and used with malicious intent.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search. The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the pupil being searched.

The authorised member of staff carrying out the search must be witnessed by a second member of staff.

There is a limited exception to this rule: Authorised staff can carry out a search of a pupil including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

The person conducting the search may not require the pupil to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the pupil has or appears to have control – this includes desks, lockers and bags.

A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

The examination of the data/files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. For guidance before taking further action staff should speak to the Headteacher.

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices.

Audit/Monitoring/Reporting/Review

The responsible person (Headteacher) will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data/files.

These records will be reviewed by the Online Safety Group annually. This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

Appendix A

Pupil Acceptable Use Agreement Template – for older students

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 access to these digital technologies.

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 students to agree to be responsible users.

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.

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 home and will not use social media in school.
- 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.)
- At home I know that I should not talk to people online unless I know them in the real world
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line to a grown up that I trust

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 act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images, use, share, publish or distribute images of others 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 bring a mobile phone to school and understand that if I do it must be handed into the school Office as soon as I arrive at 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 open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media at school.

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 online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on 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 Agreement Form

This form relates to the pupil acceptable use agreement; to which it is attached.

Please complete the sections below 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.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, google classrooms, website etc.

Name of Pupil: .....

Group/Class: .....

Signed: .....

Signature of Parent/Carer .....

Date: .....

Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation/KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet
- 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, use, share, publish or distribute images of others without their permission

Name of Chid: .....

Signed (parent/carer): .....

Date: .....

Appendix B

Parent/Carer Acceptable Use Agreement Template

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

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the pupil acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name: .....

Student/Pupil Name: .....

As the parent/carer of the above pupil/*s*, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

KS2: I know that my son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

EYFS/KS1: I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

See GDPR Policy for information on how this form will be used and stored.

Signed: .....

Date: .....

Use of Digital/Video Images- Appendix C

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name will be used.

The school will comply with the Data Protection Act and request parent's/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

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 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 pupils in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

See GDPR Policy for information on how this form will be used and stored.

Digital/Video Images Permission Form- Appendix D

Parent/Carers Name:.....Student/Pupil Name:.....

As the parent/carer of the above student/pupil, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
• to support learning activities- photos on display boards or in school	Yes/No
• on school website, class pages and gallery and in addition outside publications where appropriate e.g. Salisbury Journal	Yes/no
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Signed: .....

Date: .....

Staff (and Volunteer) Acceptable Use Policy Agreement Appendix E

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

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

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students/pupils* learning and will, in return, expect staff and volunteers 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. 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, google classrooms 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 Headteacher or Deputy Head.

I will be professional in my communications and actions when using school 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 to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/Tapestry/Google Classrooms) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use social networking sites on schools devices.
- I will not be friends with parents of children at the school on social media sites.
- I will ensure that the way I conduct myself on social media and online including communications does not harm he reputation or ethos of the school or compromise my professional responsibilities.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.

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:

- I will ensure that my mobile device is in a drawer or or cupboard so it is not accessible to children or used by me within lesson time.
- I will not use personal email addresses on the school/academy ICT systems unless in emergencies or for childcare purposes.

- 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, terrorist or extremist 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 disable or cause any damage to school/academy 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 Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal 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.
- I will look after any digital equipment that I am responsible for and acknowledge that I have a duty of care to ensure that any damage to equipment is reported straight away and that I will be liable for damage beyond reasonable wear and tear.

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 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: ----------

Appendix F- Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Appendix G- Training Needs Audit Log

Group: .....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

Appendix H Temporary Filter Removal Log

Group: .....

Date	Time	Words to be removed from filter	Information		Date removed from filter	Date to be added back to filter	Signed
			Which class	Teacher requesting			

Online Safety Group Terms of Reference- Appendix I

1. Purpose

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

2. Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group should include

- SLT member/s
- Oakford Computer support
- Governor - Safeguarding
- Parent Governor
- *Student/pupil representation* – for advice and feedback. *Student/pupil voice is essential in the make-up of the online safety group, but students/pupils would only be expected to take part in committee meetings where deemed relevant.*

2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held once a year. A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Online Safety Lead (or other relevant person) with the following :

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety.
- To ensure that monitoring is carried out of Internet sites used across the school/academy

- To monitor filtering/change control logs (e.g. requests for blocking/unBlocking sites).
- To monitor the safe use of data across the school/academy
- To monitor incidents involving cyberbullying for staff and pupils

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for St Nicholas CE (VA) Primary school have been agreed

Signed by (SLT): .....

Date: .....

Date for review: .....