Sudbourne Primary School

Online Safety Policy

This policy will be reviewed **annually** by the Resources Committee for approval by the Governing Body.

Last Review Date:	6th Nov 2020
Date Ratified by Full Governing Body:	13th Nov 2020
Next Review Date:	Nov 2021
Signature of policy approval by Headteacher:	R Blackmore (Nov 18, 2020 19:22 GMT)
Signature of policy approval by Resources Committee Chair:	Dalia Goldberg (Nov 16, 2020 12:03 GMT)
Signature of policy approval by Governing Body Chair:	Hannah Sheehan (Nov 13, 2020 20:04 GMT)

Contents

Development/Monitoring/Review of this Policy

This online safety policy has been produced and reviewed by:

- Headteacher
- Designated Safeguarding Lead
- IT Lead
- School Business Manager
- Network Manager
- Governing Board

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Governing Body on:	
The implementation of this online safety policy will be monitored by the:	*Designated Safeguarding Lead*
Monitoring will take place at regular intervals:	*Every year*
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:	*October 2021*
Should serious online safety incidents take place, the following external persons/agencies should be informed: (see Sudbourne School Safeguarding Policy for details)	*LA Safeguarding Officer* *LADO* *Police*

Scope of the Policy

This policy applies to all members of Sudbourne School's community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school/academy 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. 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 *Sudbourne 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 Sudbourne School:

Governors

Sudbourne School Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. The Governing Board's Safeguarding Governor will be the primary link between the school and the board for monitoring the school's online safety performance.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Designated Safeguarding Lead.
- The Headteacher and all members of the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see: "Responding to incidents of misuse") and relevant Lambeth Local Authority disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles.
- The Senior Leadership Team will receive regular monitoring reports from the Designated Safeguarding Lead.

Online Safety Lead (Sudbourne School's DSL)

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school technical staff
- Reports regularly to Senior Leadership Team

Network Manager/Technical staff

Sudbourne School's network is manged by an external service provider. It is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff. The managed service provider has technical responsibilities 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 Lambeth Local Authority 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
- 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 including the DSL for investigation/action/sanction
- that monitoring software/systems are implemented and updated as required

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
- they have read, understood and signed the staff acceptable use agreement
- they report any suspected misuse or problem to the Headteacher and DSL for investigation/action/sanction

- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and Acceptable Use policy
- 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

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

Pupils

- are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Agreement
- 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'* 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. Sudbourne School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, through the school website, and with information sharing 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
- their children's personal devices in school (currently not permitted)

Community Users

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign a User Acceptable Use Agreement before being provided with access to school systems.

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 and resilience 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 will be provided as part of Computing and PSHE lessons and will be regularly revisited
- Key online safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities such as circle time.
- Teachers will use daily opportunities to open up conversations with children about their internet usage and practices at home
- Pupils will 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 will be supported in building resilience to radicalisation by providing a safe environment for talking about and debating controversial issues in an age appropriate manner, and helping them to understand how they can influence and participate in decision-making
- Pupils will be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils will 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 will 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, pupils may need to research topics (e.g. racism, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their child(ren) and in the monitoring and regulation of the child(ren)'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.

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

- Letters, newsletters, school website

- Parents/carers evenings
- High profile events/campaigns e.g. Safer Internet Day

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 via 'Educare'. 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's online safety policy and acceptable use agreements.

Technical – infrastructure, equipment, filtering and monitoring

It is the responsibility of the school to ensure that the managed technical service provider carries out all the online safety measures below:

- 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 technical systems
- servers, wireless systems and cabling must be securely located and physical access restricted
- all users will have clearly defined access rights to technical systems and devices
- all users (at KS2 and above) will be provided with a username and secure password by Imran Mellick (Network Manager) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- discuss with school leaders re. suitability of group or class logons and passwords for KS1 and below, but should consider whether this models good password practice and need to be aware of the associated risks – see appendix)
- The "master/administrator" passwords for the school systems, used by the Network Manager must also be available to the School Business Manager and kept in a secure place (e.g. school safe)
- Imran Mellick (Network Manager) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content is filtered by the LGFL.
- 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. N.B. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on "appropriate filtering").
- School technical staff regularly monitor and record the activity of users on the school technical systems
- 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.

- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

Mobile Technologies

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

School owned devices only are allowed to be used in school. Personally-owned devices are not allowed to be used on school premises except in the school staff room.

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*No*	No	Staff room use only	No
Full network access	*Yes*	*Yes*	*No*	*No*	*No*	*No*
Internet Only				*No*	*Yes*	*Upon request*
No network access				*No*	*No*	*No*

School owned devices:

Staff may be loaned school owned devices to support remote working (when required). Staff will be required to complete the school IT Equipment Loan Agreement (see appendices) and must adhere to this policy.

Personal devices:

Staff, including volunteers and visitors are allowed to use personal devices in the school staff room **only**, when children are on site.

Pupils are not allowed to use personal devices of any kind on school property. Mobile phones, if brought to school, will be handed to the class teacher for safe-keeping (locked in desk). If the teacher is unable to provide this level of security, the device will be secured by school office staff.

The school will not be held responsible for any prohibited usage that results in loss/damage or malfunction following access to the school's network.

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.

- Written permission from parents/carers will be obtained as part of pupil enrolment activities relating to use of pupil images being published on the school website/social media/local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at Sudbourne School events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images. This message is shared at any events attended by parents/carers.
- 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 is not to be used for such purposes.
- 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 the school website, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. We have a school Data Protection policy that we adhere to, and an appointed Data Protection Officer (external to the school, with a high level of understanding of data protection law and is free from any conflict of interest).

- we have an information asset register in place identifying personal data held, where it is held and why, and which staff member 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
- we 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.
- we have data retention policy to ensure there are clear and understood routines for the deletion and disposal of data
- we have a school Privacy Notice in place, which provides staff, parents, volunteers, and older children with information about how the school looks after their data and what their rights with regard to this information
- we have procedures 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
- 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

- we undertake appropriate due diligence and routinely require the inclusion of data processing clauses in contracts with any data processors where personal data is processed
- we know to report any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. We know to report relevant breaches to the individuals affected as required by law.
- all staff receive data protection training at induction and appropriate refresher training thereafter relating to GDPR. 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 or removable media the:

- **data must be encrypted and password protected.**
- **device must be password protected.** (be sure to select devices that can be protected in this way)
- **device must be protected by up to date virus and malware checking software**
- **data must be securely deleted from the device, in line with Sudbourne 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 OR know which member of staff to refer such a request to.
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- 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 but must be used judiciously. When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person [Headteacher and/or Designated Safeguarding Lead], 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 must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while students/pupils at KS2 and above will be provided with individual school email addresses for educational use [if needed].

- Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

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 Sudbourne School or the 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
- Staff training provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Ensuring that staff do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions are not be attributed to the school or the 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.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy

Responding to incidents of misuse/illegal incidents

This guidance -see diagram below - 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.

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.

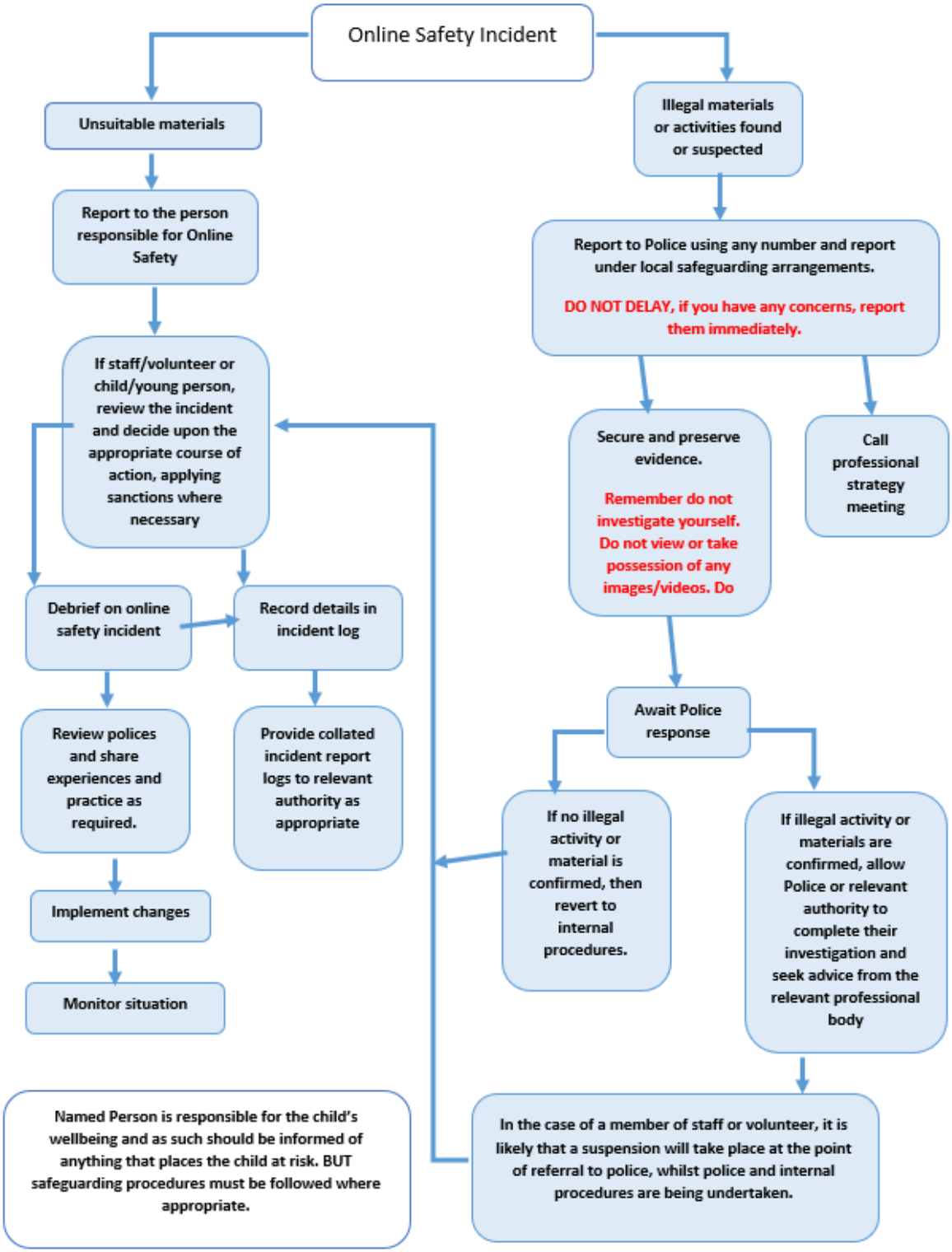
In the event of suspicion, all steps in this procedure should be followed:

- 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.
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store

screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act
    - 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 for evidence and reference purposes.


Online Safety Incident
Unsuitable materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

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	Refer to member of SLT	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning/sanctions
Deliberately accessing or trying to access material that could be considered illegal		X	X	X				
Unauthorised use of non-educational sites during lessons	X							
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device		X				X		X
Unauthorised/inappropriate use of social media/ messaging apps/personal email		X						X
Unauthorised downloading or uploading of files	X			X				
Allowing others to access Sudbourne School network by sharing username and passwords		X			X	X		X
Attempting to access or accessing the Sudbourne School network, using another student's/pupil's account		X		X	X	X		X
Attempting to access or accessing the Sudbourne School network, using the account of a member of staff			X	X	X	X		X
Corrupting or destroying the data of other users	X							
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X				X		X
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	Contact DSL		X		

Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension
Deliberately accessing or trying to access material that could be considered illegal		X	X	X		TBD by LA	
Inappropriate personal use of the internet/social media/personal email		X				X	
Unauthorised downloading or uploading of files		X			X	X	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X			X	X	
Careless use of personal data e.g. holding or transferring data in an insecure manner		X				X	
Deliberate actions to breach data protection or network security rules		X			X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X				X	
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		X	X			X	X
Actions which could compromise the staff member's professional standing		X					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X				X	
Using proxy sites or other means to subvert the school's filtering system					X		
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
Breaching copyright or licensing regulations		X			X	X	
Continued infringements of the above, following previous warnings or sanctions							X

Appendices

Pupil Acceptable Use Agreement – for KS2 pupils

Sudbourne Primary School

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/pupils* 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.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that 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 of anyone without their permission.

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

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

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.

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 Sudbourne children

Name of Pupil: .....

Class: .....

Signed: .....

Date: .....

Pupil Acceptable Use Policy Agreement (EYFS & KS1)

Sudbourne Primary School

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

Signed on behalf of child (by parent/carer): .....

Name of parent/carer: .....

Parent/Carer Acceptable Use Agreement

Sudbourne Primary School

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 *students/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: .....

Pupil Name: .....

- As the parent/carer of the above pupil, I give permission for my child to have access to the internet and to ICT systems at 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 child'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.

Signed: .....

Printed name: .....

Date: .....

Use of Digital/Video Images

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.

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.

Digital/Video Images Permission Form

Parent/Carers Name: .....

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.	Yes/No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes/No
• in the school website or newsletter	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: .....

Printed name: .....

Date: .....

Staff (and Volunteer) Acceptable Use Policy Agreement

Sudbourne Primary School

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 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, 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. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school 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) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up
- 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or student/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 to the Network Manager and School Business Manager.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to:
  - School Business Manager
  - Designated Safeguarding Lead
  - Headteacher

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 pf 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 understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's online safety policy.

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: .....

Job title: .....

Signed: .....

Date: .....

Device loan agreements for staff
Sudbourne Primary School

1. This agreement is between:

Sudbourne Primary School ("the school") and

EMPLOYEE NAME "the employee" and "I")

It governs the use and care of devices assigned to individual staff members. This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

The school is lending the employee: **1 laptop – asset ID 11658** ("the equipment") for the purpose of: **working from home.**

This agreement sets the conditions for the employee taking the equipment home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I have read and agree to these terms.

2. Damage/loss

By signing this agreement, I agree to take full responsibility for the equipment issued to me and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I am responsible for the equipment at all times whether on the school's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform ***KEMI AROGUNDADE***, **School Business Manager**, and I acknowledge that I am responsible for full replacement costs. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

School insurance, covering damage, loss or theft of equipment:

A.	Insurer	**Protector Insurance**
B.	Policy number	**528955**
C.	Inception date	**1st April 2020**
D.	Renewal date	**1st April 2021**
E.	Description	**Education Properties/contents**

3. Unacceptable use

I am aware that the school monitors my activity on the equipment.

I will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to:

- Accessing, creating, storing or linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Sharing confidential information about the school, its pupils, or other members of the school community

- Setting up any software, applications or web services on this device without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Carrying out any activity which defames or disparages the school, or risks bringing the school into disrepute
- Using inappropriate or offensive language

I accept that if I engage in any activity that constitutes 'unacceptable use', I may face disciplinary action in line with the school's policies on staff code of conduct.

4. Personal use

I will not use this devise for any personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected. This includes, but is not limited to:

- Keep the equipment password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Make sure the equipment locks automatically if left inactive for a period of time
- Do not share the equipment among family or friends
- Inform Sudbourne Tech Support if antivirus/anti-spyware software require updating
- Inform Sudbourne Tech Support if operating systems require updating

If I need help doing any of the above, I will contact ***IMRAN MELLICK, IT Network Manager*** via Technical Help remote log.

6. Return date

I will return the device in its original condition to the School Business Manager within 14 days of being requested to do so.

I will return the equipment to the school upon resignation, dismissal or if I leave the employment of the school for any other reason.

7. Consent

If staff are collecting the equipment:

By signing this form, I confirm that I have read and agree to the rules and conditions above.

PRINT FULL NAME	
SIGNATURE	
DATE	

If you cannot get a signed physical copy:

By signing this form, I confirm that I have read and agree to the rules and conditions above.

Please sign by typing your name.

FULL NAME	
DATE	

School Technical Security Policy

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 infrastructure/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 the Network Manager, Imran Mellick

Technical Security

Policy statements

The school will be responsible for ensuring that their 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 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 (if not managed by the Local Authority, these may be outlined in Local Authority/other relevant body technical/online safety policy and guidance)
- 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 systems and data
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- all users will have clearly defined access rights to the school technical systems
- details of the access rights available to groups of users will be recorded by the network manager/technical staff and will be reviewed, at least annually
- 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
- Imran Mellick, Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

(Inadequate licencing could cause the Sudbourne School to breach the Copyright Act which could result in fines or unexpected licensing costs)

- technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement
- remote management tools are used by staff to control workstations and view users activity
- an agreed policy is in procedure for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the Sudbourne School system
- *an agreed procedure is in place regarding the downloading of executable files and the installation of programmes on Sudbourne School devices by users (administrator rights are required for installing programmes).*
- 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 Sudbourne School 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 platforms).

Policy Statements:

- These statements apply to all users (except EYFS/KS1 pupils).
- 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 and will be reviewed, at least annually.
- All users (adults and KS2 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 users will be provided with a username and password by the Network Manager or the School Business Manager who will keep an up to date record of users and their usernames.

Password requirements:

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. 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 Sudbourne School
- 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 EYFS and KS1 pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. Password complexity in foundation phase will be reduced (for example 6-character maximum) and will not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.
- Password requirements for pupils at Key Stage 2 should increase as pupils progress through the school.
- KS2 pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Notes for technical staff

- 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 Sudbourne School systems should also be kept in a secure place e.g. Sudbourne 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. The should will have a minimum of network administrators will full access rights to ensure business continuity in the event of a network administrator long term absence.
- 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 Henry Canvendish Primary School IT Network Managment. *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 IT Network Manager/School Business Manager 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 by IT Network Manager/School Business Manager 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.** *(For example, your technical team may provide pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system 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 Sudbourne School's password policy:

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

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

- in lessons
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:

The responsible person (Network Manager) 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.

DfE Keeping Learners Safe in Education requires schools to have "appropriate filtering". Guidance can be found on the UK Safer Internet Centre site.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Network Manager. They will manage the school filtering, in line with this policy and 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 a second responsible person** (ICT LEAD):
- *either... be reported to and authorised by a second responsible person prior to changes being made* (SCH BUSS MGR)
- *or... be reported to a second responsible person* (ICT LEAD) *every 26 weeks in the form of an audit of the change control logs*
- *be reported to the Online Safety Group every 26 weeks in the form of an audit of the change control logs*

All users have a responsibility to report immediately to (School's ICT LEAD) 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.

- *Either - The Sudbourne School maintains and supports the managed filtering service provided by the Internet Service Provider* (LONDON GRID for LEARNING LGfL)
- *The school has provided enhanced/differentiated user-level filtering through the use of the* (JA-NET (WEBSCREEN)) *filtering programme. (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc.)*
- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher/Principal (or other nominated senior leader).*
- *Mobile devices that access the Sudbourne School internet connection (whether Sudbourne School or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *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 the technical staff* (Henry Cavendish Primary School IT Network Management)

Education/Training/Awareness

Pupils/students 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 and through online safety awareness sessions/newsletter etc.

Changes to the Filtering System

In this section the school should provide a detailed explanation of:

- Inform ICT LEAD for approval or denial of a certain site, this will be raised with IT Network Manager who are the nominated contacts with LGfL, they will insert the specific site to be included or denied within the webscreen program. The process of getting clearance on the webscreen takes less than 5 minutes to clear on the school FIREWALL.
- Two scopes on the curriculum platform can be controlled for staff and students, certain sites e.g. social media can be approved for staff and not pupils.

- WEBSCREEN is an auditing and reporting program in which all the activity within the school is constantly being monitored 24/7.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to (insert title) who will decide whether to make school level changes (as above).

Monitoring

Some schools/academies supplement their filtering systems with additional monitoring systems. If this is the case, schools/academies should include information in this section, including – if they wish – details of internal or commercial systems that are in use. They should also ensure that users are informed that monitoring systems are in place.

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 as follows:*

- Random selection of IP addresses and a detailed LOG search carried out to ensure all firewall and prevention policies are working.
- The School feels a user(s) activity is in question.

Online Safety Policy_2020 - 2021

Final Audit Report 2020-11-18

Created:	2020-11-13
By:	Kemi Arogundade (karogundade@sudbourne.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAACWf0_bC8mALMEkxj1aaU76AtF0ktRBqQ

"Online Safety Policy_2020 - 2021" History

Document created by Kemi Arogundade (karogundade@sudbourne.com)
2020-11-13 - 7:28:38 PM GMT- IP address: 5.150.102.193

Document emailed to Hannah Sheehan (hannah.sheehan@education.gov.uk) for signature
2020-11-13 - 7:29:24 PM GMT

Email viewed by Hannah Sheehan (hannah.sheehan@education.gov.uk)
2020-11-13 - 8:03:56 PM GMT- IP address: 35.176.86.207

Document e-signed by Hannah Sheehan (hannah.sheehan@education.gov.uk)
Signature Date: 2020-11-13 - 8:04:20 PM GMT - Time Source: server- IP address: 35.176.86.207

Document emailed to Dalia Goldberg (dalgol@yahoo.co.uk) for signature
2020-11-13 - 8:04:22 PM GMT

Email viewed by Dalia Goldberg (dalgol@yahoo.co.uk)
2020-11-16 - 12:01:06 PM GMT- IP address: 94.9.8.228

Document e-signed by Dalia Goldberg (dalgol@yahoo.co.uk)
Signature Date: 2020-11-16 - 12:03:44 PM GMT - Time Source: server- IP address: 94.9.8.228

Document emailed to R Blackmore (rblackmore@sudbourne.com) for signature
2020-11-16 - 12:03:46 PM GMT

Email viewed by R Blackmore (rblackmore@sudbourne.com)
2020-11-16 - 12:08:38 PM GMT- IP address: 66.249.93.75

Email viewed by R Blackmore (rblackmore@sudbourne.com)
2020-11-18 - 7:20:28 PM GMT- IP address: 213.104.127.180

Document e-signed by R Blackmore (rblackmore@sudbourne.com)
Signature Date: 2020-11-18 - 7:22:05 PM GMT - Time Source: server- IP address: 213.104.127.180

Agreement completed.

2020-11-18 - 7:22:05 PM GMT