



Mudeford Community Infants School

Online Safety Policy

Contents

| | |
|---|----|
| Introduction..... | 5 |
| Online Safety Policy..... | 6 |
| Scope..... | 6 |
| Policy development, monitoring and review..... | 6 |
| Schedule for Development/Monitoring/Review..... | 7 |
| Process for monitoring the impact of the Online Safety Policy..... | 7 |
| Roles and Responsibilities..... | 8 |
| Headteacher and Senior Leaders..... | 8 |
| Governors..... | 8 |
| Designated Safeguarding Lead..... | 8 |
| Online Safety Lead..... | 9 |
| Teaching and Support Staff..... | 10 |
| Network Manager/Technical staff..... | 10 |
| Online Safety Group (Senior Leadership Team and Safeguarding Governor)..... | 11 |
| Pupils:..... | 11 |
| Parents/carers..... | 12 |
| Community Users..... | 12 |
| Policy Statements..... | 12 |
| Education – Pupils..... | 12 |
| Education – Parents/carers..... | 13 |
| Education – The Wider Community..... | 13 |
| Use of digital and video images..... | 18 |
| Data Protection..... | 18 |
| Communications..... | 20 |
| Social Media - Protecting Professional Identity..... | 22 |
| Dealing with unsuitable/inappropriate activities..... | 23 |
| Responding to incidents of misuse..... | 26 |
| Illegal Incidents..... | 26 |
| Other Incidents..... | 28 |

| | |
|--|----|
| School actions & sanctions | 29 |
| School Online Safety Policy Appendices | 32 |
| Appendices..... | 32 |
| A) Staff (and Volunteer) Acceptable Use Policy Agreement | 33 |
| School Policy | 33 |
| This acceptable use policy is intended to ensure:..... | 33 |
| Acceptable Use Policy Agreement..... | 33 |
| For my professional and personal safety: | 33 |
| I will be professional in my communications and actions when using school systems: | 34 |
| The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the <i>school</i> : | 34 |
| When using the internet in my professional capacity or for school sanctioned personal use: | 34 |
| I understand that I am responsible for my actions in and out of the school:..... | 35 |
| B) Pupil Acceptable Use Policy Agreement..... | 36 |
| C) School Technical Security Policy (including filtering, monitoring and passwords)..... | 36 |
| Introduction..... | 36 |
| Responsibilities..... | 37 |
| Policy statements..... | 37 |
| Password Security..... | 38 |
| Policy Statements:..... | 38 |
| Learner passwords: | 39 |
| Filtering and Monitoring | 39 |
| Introduction to Monitoring..... | 40 |
| Filtering and Monitoring Responsibilities | 41 |
| DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage your filtering and monitoring systems, and include..... | 41 |
| Policy Statements..... | 42 |
| Changes to Filtering and Monitoring Systems | 43 |
| Training/Awareness: | 45 |
| Audit/Monitoring/Reporting/Review:..... | 45 |

Further Guidance..... 45

Introduction

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The Governing body should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Online Safety Policy

Scope

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

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 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Mudeford Community Infants 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.

Policy development, monitoring and review

This online safety policy has been developed by a committee consisting of:

- Headteacher
- Designated safeguarding lead (DSL)
- Staff – including teachers, support staff
- Safeguarding Governor
- Parents and carers

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development/Monitoring/Review

| | |
|---|--|
| This online safety policy was approved by the Full Governing Body on: | <i>See minutes of the FGB</i> |
| The implementation of this online safety policy will be monitored by the: | <i>Headteacher & safeguarding governor</i> |
| Monitoring will take place at regular intervals: | <i>Termly</i> |
| The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | <i>Annually in September</i> |
| The online safety policy will be reviewed annually, or more regularly in the light of significant developments in the use of technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | <i>September 2026</i> |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | <i>LA Safeguarding Officer, LADO, Police</i> |

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering

Roles and Responsibilities

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 Online Safety Lead. In this school this is currently the Headteacher.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority / other relevant body disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

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 governing body receiving regular information about online safety incidents and monitoring reports. The safeguarding governor has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Leader
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting at relevant Governors meetings

Designated Safeguarding Lead

Keeping Children Safe in Education states that:

“The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder’s job description.”

They (the DSL) “are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college”

They (the DSL) “can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online”

While the responsibility for online safety is held by the DSL and cannot be delegated, the school may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities. It is recommended that the school reviews the sections below for the DSL and OSL and allocate roles depending on the structure it has chosen

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor (safeguarding) to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)
- Will 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 Lead

- leads the Online Safety Group
- 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
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online Safety Governor (safeguarding governor) to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors
- reports as necessary to Senior Leadership Team

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 policy/agreement (AUP/AUA)
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with learners, parents and carers and others should be on a professional level and only carried out using official school systems and devices, where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements
- they immediately report any suspected misuse or problem to the Headteacher Leader (Online Safety Lead) for investigation/action/sanction
- 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 at an age appropriate level
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (at a basic age appropriate level for EYFS/KS1)
- 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
- they adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

Network Manager/Technical staff

The school has a managed ICT service provided by an outside contractor - Coretek, 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, as suggested below. It is also important that the managed service provider is fully aware of the school online safety policy and procedures.

Those with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack

- that the school meets required online safety technical requirements and any Local Authority online safety policy/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” 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 (Online Safety Lead) for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Online Safety Group (Senior Leadership Team and Safeguarding Governor)

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production/review/monitoring of the school online safety policy/documents.
- the production/review/monitoring of school filtering and requests for filtering changes.
- 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

Pupils:

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (at a basic age appropriate level for EYFS/KS1)
- 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, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line pupil records
- their children's personal devices in the school (where this is allowed). At this school there is no necessity for personal devices and so they are 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 Community User Acceptable Use Agreement (AUA) before being provided with access to school systems. This is not applicable to our school.

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 as appropriate and staff should reinforce online safety messages across the curriculum in an age appropriate way and as necessary in accordance with the subject matter. 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 and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral 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 taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. 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.
- Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils or staff 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 the Technical Support Provider (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. [swgfl.org.uk](http://www.swgfl.org.uk), www.saferinternet.org.uk, <http://www.childnet.com/parents-and-carers>

Education – The Wider Community

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

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision

- **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. 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/academy online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead 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 / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents.

Technical – infrastructure/equipment, filtering and monitoring

The school has a managed ICT service provided by an outside contractor (Coretek), 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, as suggested below. It is also important that the managed service provider is fully aware of the school online safety policy/acceptable use agreements. The school should also check their Local Authority other relevant body policies on these technical issues.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure

that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the school office (this is generated by Coretek who will keep an up to date record of staff users and their usernames). Pupil records are held by the school office in the secure Admin drive or via a secure cloud based online system (such as SIMS / Google Classroom).
- Users are responsible for the security of their username and password. The “master/administrator” passwords for the school/academy 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
- Coretek and / or school admin staff 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 by actively employing the Internet Watch Foundation Child Abuse Images and Content (CAIC) list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. Requests are made to the headteacher who will then instruct relevant staff members.
- **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 computing lead monitors (and records if/when necessary) the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the headteacher. Staff to report verbally or via email.
- 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. They sign to say they have agreed to confidentiality and safeguarding procedures outlined in the visitors and work placement booklet.
- An agreed policy is in place regarding the extent of personal use that users (staff/ pupils) and their family members are allowed on school devices that may be used out of school. Staff members may use school devices for personal use that excludes social media (unless for educational purposes such as following educational consultants and webinars on Twitter etc) and online gaming. The viewing of news, email, browsing the internet, shopping, viewing online streaming services is permitted within the boundaries of legal and appropriate content.

- An agreed policy is in place regarding the use of removable media by users on school devices. **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.**

Mobile Technologies (including Bring your own device/technology BYOD/BYOT)

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 which may include the school’s learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s online safety education programme.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include: security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership.

- **The school acceptable use agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies**
- **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 | Yes | No ² | Yes ² | Yes |
| Full network access | Yes | Yes | Yes | No | No | No |
| Internet only | | | | No | Yes | Yes |

Aspects that the school may wish to consider and be included in their online safety policy, mobile technologies policy or acceptable use agreements:

¹ Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

² The school should add below any specific requirements about the use of mobile/personal devices in school

School owned/provided devices:

- Are allocated to individual staff members / groups / classes / individual children for remote learning purposes only
- School devices may be used on school premises and out of school (to be signed out on each occasion). Pupils are to use devices for educational purposes only.
- Personal use is permitted within the boundaries of legal and appropriate content.
- Staff may manage devices / apps / changing of settings as appropriate and in line with appropriate content and security systems recognising that this will be monitored
- Technical support is provided by Coretek for which staff members have access to contact details
- School filtering services operate on school premises. No harmful or inappropriate material should be installed / downloaded / viewed at any time on a school device
- Users have access to relevant cloud services such as Apple / Google / Microsoft
- Users must adhere to data protection policy and procedures at all times and report a breach to the headteacher.
- Taking/storing and using images of children is permitted for educational purposes only. All devices are password protected and all images should not be shared with anyone outside of school without relevant permission from parents. All images should be removed / deleted from the device once they have been used. If the storing of images is required, then these should be saved onto the secure school server and then the images should be immediately removed.
- If necessary, staff devices will be restored to factory settings upon them leaving the school.
- Liability for damage remains with the school unless there is evidence of deliberate mistreatment resulting in the staff disciplinary policy being applied.
- Staff will be trained and given guidance on how to use devices appropriately

Personal devices:

- Unless there are exceptional circumstances of which the headteacher has been notified, personal mobile devices must not be used when in any proximity to children by staff / pupils / visitors
- Staff should only use personal mobile devices in designated staffrooms or offices or when there are no children in proximity.
- Visitors must only use mobile phones as a necessity and not without the permission of the accompanying member of staff. Visitors must never use mobile phones when in proximity of children unless permission has been sought by a member of staff and they are accompanied whilst doing so or taken to a private room.
- Mobile personal devices should not be kept on person unless permission has been given by the headteacher or senior leader. They should be packed away securely.
- Staff may use personal devices for school business but should withhold their personal number at all times when in contact with parents or other unsuitable / inappropriate contacts.
- No technical support is available for personal mobile devices
- Filtering of the internet connection to personal mobile devices are in line with school systems
- When using personal mobile devices Data Protection policy and procedures must be adhered to at all times.
- The school will not be held responsible or liable for loss/damage or malfunction following access to the network.

- Visitors will be informed about school requirements of personal mobile device use upon entry to the school.
- Education about the safe and responsible use of mobile devices is included in the school online safety education programmes and staff training.
-

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 students/pupils are published on the school website/social media/local press.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff 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.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. Schools should ensure that they take account of policies and guidance provided by local authorities or other relevant bodies.

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

The school 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) a level of understanding of the data protection law commensurate with its applicability to our school, is free from any conflict of interest and knowledge of how to obtain relevant legal advice. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- 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, volunteers, with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- 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 or removable media the:

- data must be encrypted and password protected.
- devices must be password protected.
- devices 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 understand 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 (including USBs) these must be encrypted and password protected. Avoid using USB devices for storage of personal data unless absolutely necessary.
- will not transfer any school personal data to personal devices 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:

| | Staff & other adults | | | | Pupils | | | |
|---|----------------------|--------------------------|----------------------------|-------------|-------------|---------|--------------------------|-------------------------------|
| | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission |
| Communication Technologies | | | | | | | | |
| Mobile phones may be brought to the school | X | | | | X | | | |
| Use of mobile phones in lessons | | | | X | 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 | X | | | | X | | | |
| Use of social media | | X | | | X | | | |
| Use of blogs | | | | | X | | | |

When using communication technologies, the school/academy 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 – 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, Virtual Learning Environment (VLE) etc) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1. (Schools/academies may choose to use group or class email addresses for younger age groups e.g. at KS1)

- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
-

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how a school protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

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
- Risk assessment, including legal risk

School staff should ensure that:

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

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

- A process for approval by senior leaders

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

Personal Use:

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

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments whereby the Headteacher would engage with SLT and the safeguarding governor to agree an approach.
- The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|--|------------|-----------------------------|--------------------------------|--------------|--------------------------|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images sexting – <u>UKSIC Responding to and managing sexting incidents</u> and <u>UKCIS – Sexting in schools and colleges</u> | | | | | 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: | | | | | | |
| <ul style="list-style-type: none"> Gaining unauthorised access to school networks, data and files, through the use of computers/devices Creating or propagating computer viruses or other harmful files | | | | | | X |

- 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 prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information [here](#)

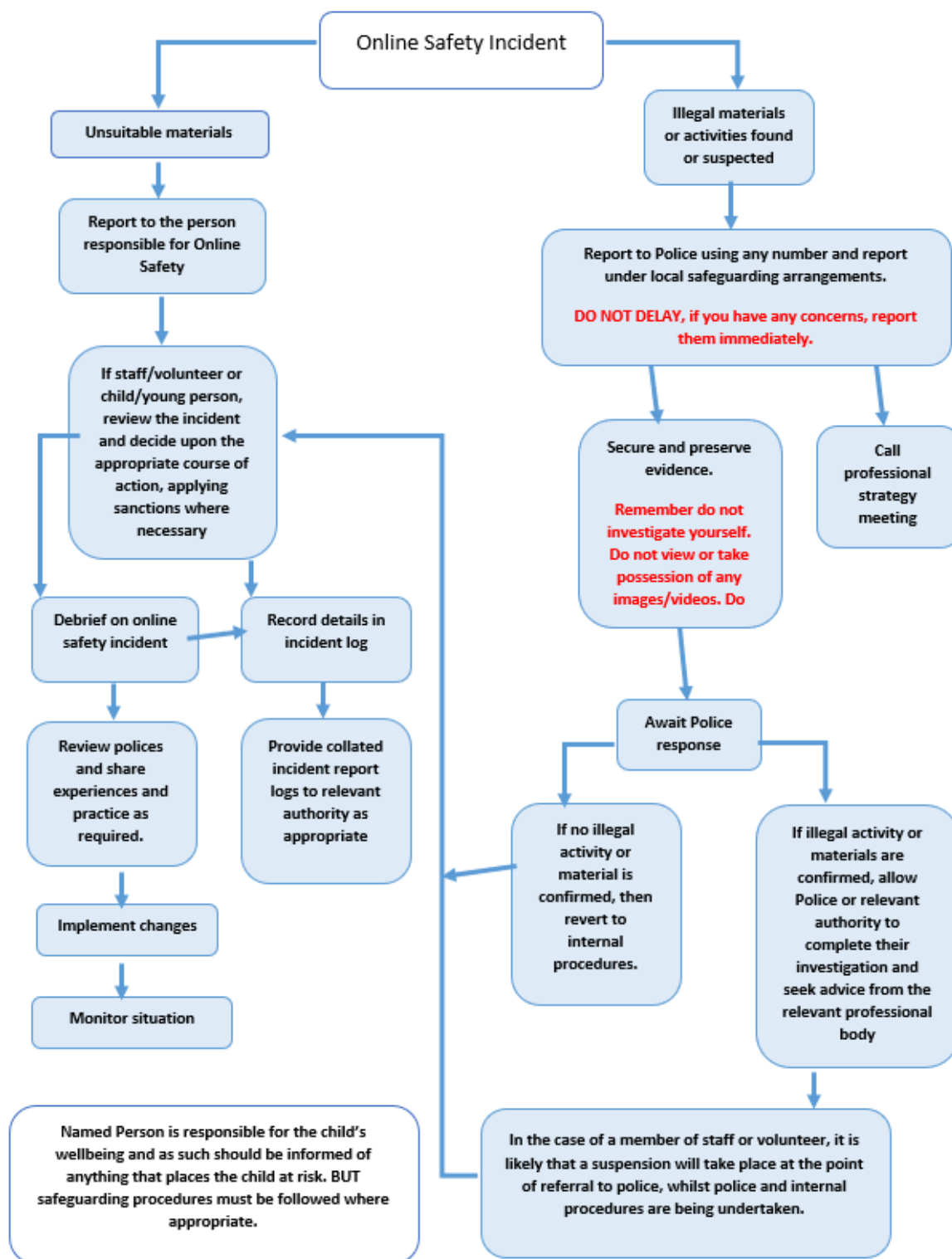
| | | | | | |
|--|---|---|--|---|--|
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy | | | | X | |
| Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, 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) as instructed by staff member | x | | | | |
| On-line gaming (non-educational) – appropriately selected by staff member | | x | | | |
| On-line gambling | | | | x | |
| On-line shopping/commerce – staff only | | x | | | |
| File sharing – staff only unless pupil supervised | x | | | | |
| Use of social media – when appropriate to do so for communications and educational purposes | | x | | | |
| Use of messaging apps – by staff members only for communication with staff and relevant outside agencies | | x | | | |
| Use of video broadcasting e.g. Youtube – for appropriate communications to stakeholders | | 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 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 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 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:

| Pupils Incidents | Actions/Sanctions | | | | | | | | |
|---|------------------------|------------------------|----------------------|-----------------|--|-----------------------|---|---------|---|
| | Refer to class teacher | Refer to Senior Leader | 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 | 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 | 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 | | X | |
| Unauthorised/inappropriate use of social media/messaging apps/personal email | | X | 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 | | 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 | X | |
| Corrupting or destroying the data of other users | X | X | X | | | X | X | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | X | | | 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 | 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 | 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 | X | |

Actions/Sanctions

| Staff Incidents | Refer to line manager | Refer to Headteacher Principal | Refer to Local Authority/HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc. | Warning | 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 | | X | X | X |
| Inappropriate personal use of the internet/social media/personal email | | X | X | | | 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 | | | X | | X |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | X | X | | | | X | | |
| Deliberate actions to breach data protection or network security rules | X | X | X | | | X | | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | X | X | X | X | | X | | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | X | X | | X | X | X |
| Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils | X | X | X | | | X | | X |
| Actions which could compromise the staff member's professional standing | X | X | X | | | X | | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | X | X | | | 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 | | | X | | X |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | X | | | X | X | X |
| Breaching copyright or licensing regulations | X | X | | | | X | | |
| Continued infringements of the above, following previous warnings or sanctions | | X | X | | | X | X | X |

School Online Safety Policy

Appendices

Appendices

- A) Staff (and Volunteer) Acceptable Use Policy Agreement 33
- B) Pupil Acceptable Use Policy Agreement 36
- C) School Technical Security Policy (including filtering, monitoring and passwords) 36

A) Staff (and Volunteer) Acceptable Use Policy Agreement

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 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, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school as per the online safety policy.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

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

- When I use my 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 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/ LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based 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.

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/academy digital technology equipment in school, but also applies to my use of school/academy 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/academy
- 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:

B) Pupil Acceptable Use Policy Agreement

To be managed through Arbor using the following statements

- The pupil will ask a teacher or suitable adult if they want to use the computers/tablets
- The pupil will only use activities that a teacher or suitable adult has told or allowed them to use
- The pupil will take care of computers/tablets and other equipment
- The pupil will ask for help from a teacher or suitable adult if they are not sure what to do or if they think they have done something wrong
- The pupil will tell a teacher or suitable adult if they see something that upsets them on the screen
- The pupil will know that if they break (do not follow) the rules they might not be allowed to use a computer/tablet
- The pupil will not share their name, address, or pictures
- The pupil will be kind when using technology, just like they are in real life.
- The teacher or suitable adult will monitor what the pupil does on computers, tablets and the internet to keep me safe.

These rules help us all stay safe and have fun using computers and tablets at school!

C) School Technical Security Policy (including filtering, monitoring and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. This is informed by the

Department for Education (DfE) guidance, Keeping Children Safe in Education, and the Digital and Technology Standards and therefore applicable for schools and colleges in England. For schools and colleges outside England, this would be considered good practice, the school should also ensure that they remain compliant with national, local authority or MAT guidance, as relevant. The school is 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
- access to personal data is securely controlled in line with the school's personal data policy
- system logs are maintained and reviewed to monitor user activity
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems, including filtering and monitoring provision

Responsibilities

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. The management of technical security is the responsibility of Governors and Senior Leaders, supported in this by the Designated Safeguarding Lead, Online Safety Lead and IT Service Provider.

Policy statements

The school is 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/MAT, these may be outlined in Local Authority/other relevant body technical guidance)
- cyber security is included in the school risk register.
- 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.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- appropriate security measures (including updates) are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from

accidental or malicious attempts which might threaten the security of the school systems and data, including operating systems.

- the school's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.
- 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 school technical systems and accounts are deleted when the user leaves. *Details of the access rights available to groups of users will be recorded by the network manager/technical staff/other person 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
- The IT Service Provider, in partnership with Governors/SLT/DSL, regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- mobile device security and management procedures are in place
- an appropriate system is in place whereby staff report via email directly to the headteacher for users to report any actual/potential technical incident
- Coretek 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
- by default, users do not have administrator access to any school-owned device
- personal data cannot be sent over the internet or taken off the 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 platform)..

Policy Statements:

- The password policy and procedures reflect NCSC and DfE advice/guidance.
- The use of passwords is reduced wherever possible, for example, using Multi-Factor Authentication (MFA) or (Single Sign On) SSO.
- Security measures are in place to reduce brute-force attacks and common passwords are blocked.
- School networks and system will be protected by secure passwords.
- Passwords are encrypted by the system to prevent theft.
- Passwords do not expire and the use of password managers is encouraged.
- Complexity requirements (e.g. capital letter, lower case, number, special character) are not used.
- Users are able to reset their password themselves.

- All passwords are at least 12 characters long and users are encouraged to use 3 random words.
- Passwords are immediately changed in the event of a suspected or confirmed compromise.
- No default passwords are in use. All passwords provided "out of the box" are changed to a unique password by the IT Service Provider.
- All accounts with access to sensitive or personal data are protected by Multi-Factor Authentication methods when used on personal devices outside of school. Admin staff, pastoral leader and SLT are the only staff members
- A copy of administrator passwords is kept in a secure location.
- All users (adults and learners) 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.

Learner passwords:

Schools need to take a risk-based approach to the allocation of learner usernames and passwords. Schools should be able to identify individuals accessing their systems and an individual logon is the recommended approach. For younger children and those with special educational needs, the DfE guidance states that schools could:

- consider using authentication methods other than passwords.
- consider using a separate account accessed by the teacher rather than the student.
- segment the network so such accounts cannot reach sensitive data.
- consider if the data or service being accessed requires authentication.

Policy Statements

- The learners at Mundeford Community Infants School do not have individual accounts, none of the applications they use allow saving of data.

Filtering and Monitoring

Introduction to 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, as online content 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. Many users are not aware of the flexibility provided by many filtering services at a local level for schools. Where available, schools should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies. Provide training and awareness raising to help users understand the process that is available to them.

DfE Keeping Children Safe in Education requires schools to have “appropriate filtering”. DfE published Filtering and monitoring standards for schools and colleges in March 2023. Schools are recommended to use the UK Safer Internet Centre Definitions to help them determine if their filtering system is appropriate.

Schools may wish to test their filtering for protection against illegal materials at: [SWGfL Test Filtering](#)

Your filtering system should be operational, up to date and applied to all:

- users, including guest accounts.
- school owned devices
- devices using the school broadband connection.

Your filtering system should:

- filter all internet feeds, including any backup connections.
- be age and ability appropriate for the users and be suitable for educational settings.
- handle multilingual web content, images, common misspellings and abbreviations.
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.
- provide alerts when any web content has been blocked.

Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

Introduction to Monitoring

Monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows you to review user activity on school and college devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

Your monitoring strategy should be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

DfE Keeping Children Safe in Education requires schools to have “appropriate monitoring”. DfE published Filtering and monitoring standards for schools and colleges in March 2023. Schools are recommended to use the UK Safer Internet Centre Definitions to help them determine if their monitoring system is appropriate

Filtering and Monitoring Responsibilities

DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage your filtering and monitoring systems, and include

| Role | Responsibility | Name / Position |
|------------------------------|--|-----------------|
| Responsible Governor | Strategic responsibility for filtering and monitoring and need assurance that the standards are being met. | |
| Senior Leadership | <p>Team Member Responsible for ensuring these standards are met and:</p> <ul style="list-style-type: none"> • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports <p>Ensure that all staff:</p> <ul style="list-style-type: none"> • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns | |
| Designated Safeguarding Lead | Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: | |

| | | |
|--|--|--|
| | <ul style="list-style-type: none"> • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems | |
| IT Service Provider | <p>Technical responsibility for:</p> <ul style="list-style-type: none"> • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems | |
| <p>All staff</p> <p>need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:</p> | <ul style="list-style-type: none"> • they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material | |

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 URL 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.

- There is a filtering and monitoring system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content.
- There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.
- Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.

- The filtering and monitoring provision is reviewed at least annually and checked regularly.
- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change.
- Mobile devices that access the school's internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.
- The school has provided enhanced/differentiated user-level filtering through the use of the RM filtering system. (allowing different filtering levels for different ages/stages and different groups of users – staff/learners etc.)

Changes to Filtering and Monitoring Systems

There should be a clear process for requests to change the filtering and monitoring systems and who makes the decision to alter the filtering system.

Filtering and Monitoring Review and Checks

To understand and evaluate the changing needs and potential risks of the school, the filtering and monitoring provision will be reviewed at least annually. The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider. Additional checks to filtering and monitoring will be informed by the review process so that governors have assurance that systems are working effectively and meeting safeguarding obligations.

Reviewing the filtering and monitoring provision

A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of learners and staff.

The review will take account of:

- the risk profile of learners, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of learners
- teaching requirements, for example, the RHSE and PSHE curriculum
- the specific use of chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies are in place
- what checks are currently taking place and how resulting actions are handled

To make the filtering and monitoring provision effective, the review will inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review will be carried out as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, e.g. remote access or BYOD
- new technology is introduced

Checking the filtering and monitoring systems

Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

When filtering and monitoring systems are checked this should include further checks to verify that the system setup has not changed or been deactivated. Checks are performed on a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

Logs of checks are kept so they can be reviewed. These record:

- when the checks took place
- who did the check
- what was tested or checked
- resulting actions

The SWGfL Filtering Standards checklist may be helpful.

Training/Awareness:

It is a statutory requirement in England that staff receive training, at least annually, about safeguarding, child protection, online safety and filtering and monitoring. Furthermore, in order to protect personal and sensitive data, governors, senior leaders, staff and learners should receive training about information security and data protection, at least annually.

Governors, Senior Leaders and staff are made aware of the expectations of them:

- at induction
- at whole-staff/governor training
- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring (Responsible Governor, DSL, OSL or other relevant persons) will receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

Learners are made aware of the expectations of them:

- in lessons
- through the acceptable use agreements

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

Audit/Monitoring/Reporting/Review:

Governors/SLT/DSL/OSL will ensure that full records are kept of:

- Training provided
- User Ids and requests for password changes
- *User logons*
- *Security incidents related to this policy*
- *Annual online safety reviews including filtering and monitoring*
- *Changes to the filtering system*
- *Checks on the filtering and monitoring systems*

Further Guidance

Schools may wish to seek further guidance. The following is recommended:

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"*. Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to *"ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's 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."* Ofsted concluded as far back as 2010 that "Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves."

To further support schools and colleges in England, the Department for Education published Digital and Technology standards.

The UK Safer Internet Centre has produced guidance on ["Appropriate Filtering and Monitoring"](#)

SWGfL, on behalf of UK Safer Internet Centre and DfE, developed further Filtering and Monitoring | SWGfL information for schools and colleges, including a checklist alongside further support for Governors

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