



# FOUNTAINS PRIMARY SCHOOL

Always achieving our potential

## Online Safety Policy

Written: April 2023

To be reviewed: April 2024

Policy Owner: Mr Dan Richins (Online Safety Lead)

Mrs Abi Wilburn (Computing Lead)

Mrs Alison Revill and Mrs Laura Kobylanski (DSLs)

Ratified: Mrs Nicola Price (Headteacher)



ALWAYS ACHIEVING OUR POTENTIAL



## Introduction

Fountains Primary School is responsible for ensuring that the school infrastructure 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.

There will be regular reviews and audits of the safety and security of Fountains Primary School technical systems:

- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to Fountains Primary School technical systems. Details of the access rights available to groups of users will be recorded by Technical Staff and will be reviewed, at least annually, by the Online Safety Committee.
- 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.
- Technical 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 licenses purchased against the number of software installations
- Mobile device security and management procedures are in place.
- The Designated Safeguarding Lead and Online Safety Lead actively monitor and record the activity of users on the school technical systems through Securix active Monitoring and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual / potential technical incident to the Online Safety Coordinator / Technician/ Senior Leadership Team.
- The Acceptable Use Policy discusses the downloading of executable files and the installation of programs on school devices by users
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see Esteem MAT Data Protection Policy 2022-2025)

## Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

## Headteacher and Senior Leaders

The Headteacher and Senior Leaders have a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.

The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, Designated Safeguarding leads, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

They will ensure that the Securix active monitoring system and Netsweeper filtering is in place, allowing appropriate filtering and monitoring support to those in school who carry out the internal monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. The headteacher/senior leaders will receive monitoring reports from the Online Safety Lead of Grade 4/5 violation captures or reports of unauthorised access to restricted content.

The headteacher and 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.

## Designated Safeguarding Lead (DSL)

The DfE guidance “Keeping Children Safe in Education 2022” states:

- “The designated safeguarding lead should take lead responsibility for safeguarding and child protection (**including online safety**). This should be explicit in the role holder’s job description.” ... Training should provide designated safeguarding leads with a good understanding of their own role, ... so they ... 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.”

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming

The role of DSL will also include:

- being aware of the potential for serious child protection concerns
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- liaises with the local authority/MAT/relevant body on safeguarding (including Online Safety) issues

## Online Safety Lead (CEOP Ambassador)

The role of Online Safety Lead will also include:

- work closely with the Designated Safeguarding Lead (DSL) to take day-to-day responsibility for online safety issues
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- report regularly to headteacher/senior leadership team

## Governors

The DfE guidance “Keeping Children Safe in Education 2022” states:

- “Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children’s welfare .... this includes ... online safety”

Governors are responsible for the approval of the Safeguarding Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document “Online Safety in Schools and Colleges – questions from the Governing Body”.

The named Safeguarding Governor will also oversee the role as Online Safety Governor and will receive information about online safety incidents and monitoring reports. The role will also include:

- regular meetings with the DSL and/or Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting to relevant governors group/meeting
- invited to be a member of the school Online Safety Committee and attend half termly meeting
- occasional review of the filtering change control logs and the monitoring of filtering logs (where possible)

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

## Computing Curriculum Lead

Curriculum Lead for Computing will work with the Designated Safeguarding Lead and Senior Leaders to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE and National Online Safety

This will be provided through:

- a bespoke programme accessible for each curriculum pathway
- PHSE and SRE programmes (Jigsaw)
- A mapped cross-curricular programme
- assemblies and pastoral programmes

- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

## Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the Staff/Volunteer Acceptable Use Policy 2022-2023 (AUP)
- they immediately report any suspected misuse or problem to the Online Safety Lead, DSL or Senior Leaders for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems outlined in the Staff Code of Conduct 2022-2023
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and Acceptable Use Policy, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

## Professional Standards – Code of Conduct 2022-2023

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

## Online Safety Committee

The Online safety Committee provide a consultative group that has wide representation from the Fountains Primary School community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. The group is made up of class elected representatives with support from the Headteacher/Senior Leaders, the Online Safety Lead, parents/carers and online safety governor are also invited to attend.

The committee will assist the Online Safety Lead and Senior Leaders with

- the production/review/monitoring of the school Online Safety Policy
- the monitor requests for filtering changes

- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

## Pupils (Where appropriate)

- where appropriate, are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy 2022-2023 which they will be expected to sign (or signed on their behalf by an adult who has Parental Responsibility for that child) before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology (poster were developed by the school council and are displayed around school)
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking and use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school

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

Online safety education will be provided in the following ways:

- A planned online safety programme is provided as part of Computing, PSHE, extended learning (afterschool/ lunchtime clubs) and other lessons. This should be regularly revisited - this will cover both the use of ICT and new technologies in school and outside school
- Key online safety messages should be reinforced as part of a planned programme of assemblies, tutorial, pastoral activities and activity weeks.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems and the internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

## Parents and carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and any mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through consultation days, newsletters, letters, website links, information about national and local online safety campaigns, inviting parents to join the online safety committee, discussions during parent forum meetings.

Some parents and carers may only have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. 'There is a generational digital divide'. (Byron Report).

Fountains Primary School will take every opportunity to help parents and carers understand these issues through:

- Inviting parents and carers to Parent Forum meetings with an Online Safety focus
- publishing the school Online Safety Policy on the school website
- asking parents/carers to acknowledge the parent/carer and pupil Acceptable Use Policies by signature
- publishing information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning the use of their child's digital images/video
- half termly newsletters updates, regular online safety updates to the website, social media and information about national/local online safety campaigns and literature

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school

## Online Safety Policy

The DfE guidance “Keeping Children Safe in Education” states:

- “Online safety and the school or college’s approach to it should be reflected in the child protection policy”

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and is published on the school website.

## Acceptable Use Policies

Fountains Primary School has defined what it regards as acceptable/unacceptable use and the Staff and Volunteer Acceptable Use Policy 2022-2023 and the Parent/Carer and pupil Acceptable Use Policy 2022-2023.

These documents outlines the school’s expectations on the responsible use of technology by its users. They are signed or acknowledged by all staff as part of their conditions of employment. Where appropriate, pupils and parents/carers them, though it is more important for these to be understood and followed rather than just signed.

The acceptable use agreements are re-enforced through:

- staff induction and code of conduct
- splash screens on sign in
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- peer support

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

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community



- users should immediately report to a 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
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

## Reporting and responding

The 2021 Ofsted “Review of Sexual Abuse in Schools and Colleges” highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:


*“School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:*

- *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse”*

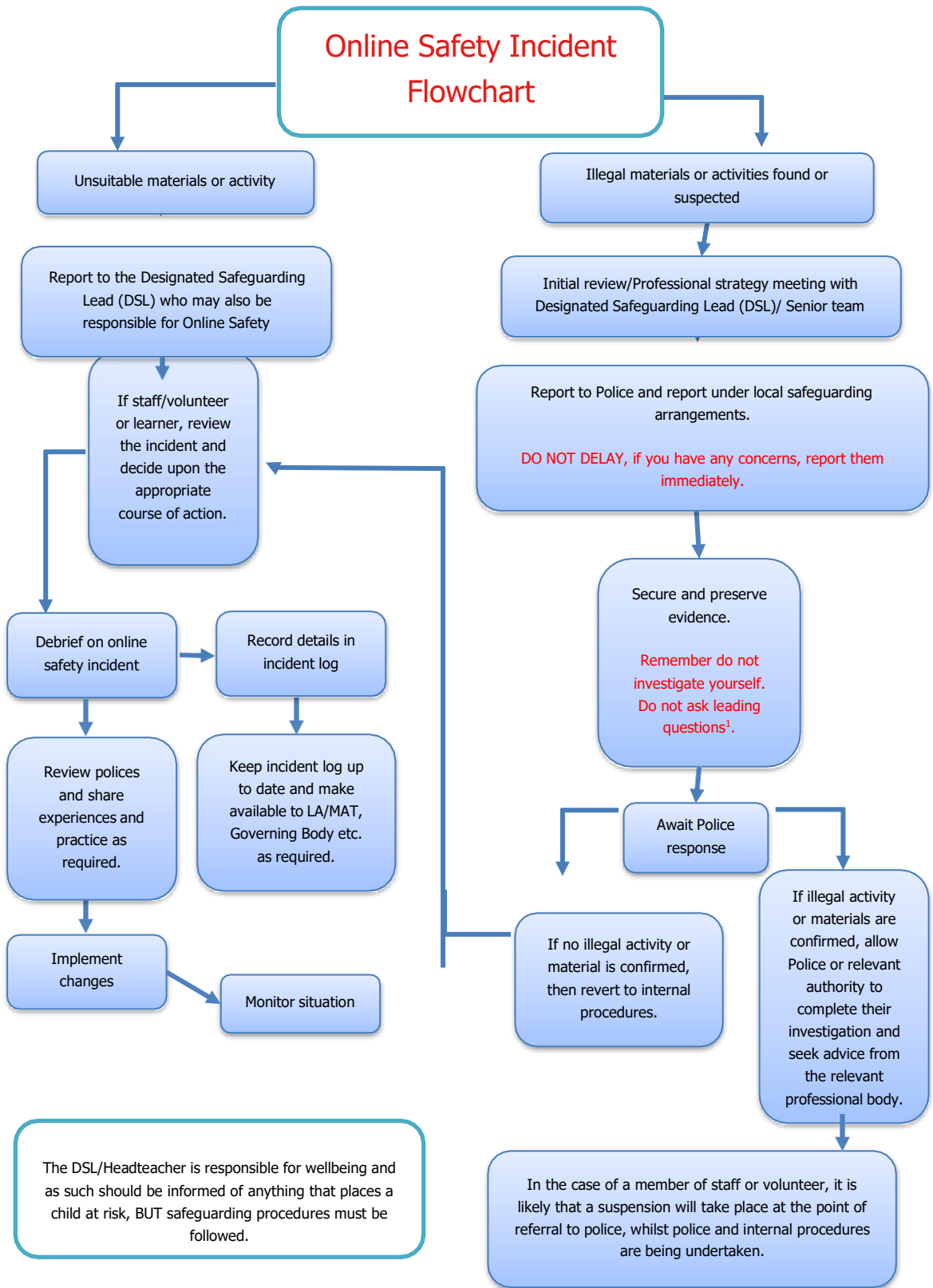
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority / MAT
- where there is no suspected illegal activity, devices may be checked using the following procedures:

- one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- ensure that the relevant staff 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
- 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 / MAT (as relevant)
  - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged using MyConcern
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; [Professionals Online Safety Helpline](#); [Reporting Harmful Content](#); [CEOP](#).
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided to:
  - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
  - *staff, through regular briefings*
  - *learners, through assemblies/lessons*
  - *parents/carers, through newsletters, school social media, website*
  - *governors, through regular safeguarding updates*
  - *local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested “working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour”*



The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



## School actions

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.

## Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

*"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."*

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Pupils needs and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners on different curriculum pathways
- pupils should be helped to understand the need for the pupils acceptable use policy 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 learners 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 learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of 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
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

## Contribution of Pupils

Fountains Primary School acknowledges, learns from, and uses the skills and knowledge of pupils in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass pupil feedback and opinion.
- the Online Safety Committee has class elected representative from all curriculum pathways
- pupils contribute to the online safety education programme e.g. peer education, committee members distributing online safety information and campaigns
- pupils designing/updating acceptable use policies and posters
- contributing to online safety events with the wider school community e.g. parents' evenings, online safety day, online safety drama workshop etc.

## Staff/volunteers

The DfE guidance "[Keeping Children Safe in Education](#)" states:

"All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."

"Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning."

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Staff are required to complete Annual Certificate in Online Safety for Education Settings, a CPD approved formal online safety training from the National College. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- The Online Safety Lead as CEOP Ambassador will annually deliver Child Exploitation Online Protection Training.
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- The Designated Safeguarding Lead, Computing Lead and Online Safety Lead will receive regular Online Safety updates and bulletins.
- This Online Safety Policy and its updates will be presented and distributed to all staff.
- The Online Safety Lead will provide advice, guidance and training as required to individuals as required.

## Governors

Governors should take part in online safety training/awareness sessions, with particular importance to the Safeguarding Governor who is also responsible for Online Safety. This may be offered in several ways such as:

- attendance at training provided by Esteem MAT or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor.

## Wider Community

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

- online safety messages targeted towards families and relatives.
- providing family learning courses in use of digital technologies and online safety via National Online Safety or Parent/Carer forum sessions
- the school will provide online safety information via their website and social media for the wider community

# Technology

## Filtering

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. Filtering is provided by Netsweeper and meets the standards defined in the UK Safer Internet Centre [Appropriate filtering](#).
- access to online content and services is differentiated and managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes
- the school has differentiated user-level filtering (allowing different filtering levels for different groups of users: pupil, pupil+, staff, staff+ etc.)
- younger learners will use child friendly/age-appropriate search engines e.g. [SWGfL Swiggle](#)
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL [Report Harmful Content](#) site, the button for 'Harmful Material - Lawful but Awful' is now displayed on [www.fountainsprimaryschool.co.uk](http://www.fountainsprimaryschool.co.uk) website footer along with report CEOP button.

## Monitoring

The DfE guidance "[Keeping Children Safe in Education](#)" states:

"It is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the ... risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff



have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. “

The school has active Securus monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its laptop and desktop services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored via the AUP. The Online Safety Lead and ICT Manager is responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment. These may include:

- physical monitoring of iPads (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems

## Technical Security

The 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 are 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 using RedStor
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT Manager and Technician and will be reviewed, at least annually, by the Online Safety Committee
- all users (adults and pupils) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security

- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password the IT Manager or Technician who will keep an up-to-date record of users and their usernames
- the master account passwords for the school systems are kept in a secure place, e.g. school safe.
- passwords should be long and strong
- records of pupil usernames and passwords can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- [the IT Manager and Technician](#) are responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- any actual/potential technical incident/security breach must be reported to the IT Manager, Technician or Senior Leaders
- appropriate security measures are in [place](#) to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software from Sophos and is managed by Entrust Learning Technologies.
- an acceptable use policy is in place that forbids staff from downloading executable files and installing programmes on school devices
- an acceptable use policy and data protection policy is in place regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

## Mobile Technologies

The DfE guidance “Keeping Children Safe in Education” states:

*“The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.*”

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, 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 services and other cloud-based services such as e-mail and datastorage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies guidance should be consistent with and inter-related to other relevant school policies including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and conduct. 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 learners
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

The school acceptable use policies for staff, pupils, parents, and carers outline the expectations around the use of mobile technologies.

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device <sup>1</sup>	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only				No	Yes	Yes
Network access				No	No	No

### School owned/provided devices:

- to whom they will be allocated
- where, when and how their use is allowed – times/places/in/out of school
- if personal use is allowed

---

- levels of access to networks/internet (as above)
- management of devices/installation of apps/changing of settings/monitoring
- network/broadband capacity
- technical support
- filtering of devices
- access to cloud services
- use on trips/events away from school
- data protection
- taking/storage/use of images
- exit processes, what happens to devices/software/apps/stored data if user leaves the school
- liability for damage
- staff training.

## Personal devices

- which users are allowed to use personal mobile devices in school (staff/learners/visitors)
- restrictions on where, when and how they may be used in school
- if used in support of learning, how staff will plan their lessons around the potential variety of device models and different operating systems
- storage
- whether staff will be allowed to use personal devices for school business
- levels of access to networks/internet (e.g., access, or not, to internet/guest wi-fi/network)
- network/broadband capacity
- technical support
- filtering of the internet connection to these devices and monitoring the access
- management of software licences for personally owned devices.
- data protection
- taking/storage/use of images
- liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility)
- identification/labelling of personal devices
- how visitors will be informed about school requirements
- how education about the safe and responsible use of mobile devices is included in the school online safety education programmes
- how misuse will be dealt with

## Social Media

Expectations for teachers' professional conduct are set out in the [DfE Teachers Standards](#) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

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

Reasonable steps to prevent predictable harm must be in place.

**Fountains Primary School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils through:**

- ensuring that personal information is not published
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk
- guidance for learners, parents/carers

**School staff should ensure that:**

- no reference should be made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

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

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- 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, 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 personal social media sites during allocated lunch break.

## Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school
- the school should effectively respond to social media comments made by others according to a defined policy or process
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the [Professionals Online Safety Helpline](#).

## Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

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

- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- 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 / academy 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 / academy into disrepute.
- 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 without permission
- Named pupil's work can only be published with the permission of the pupil and parents or carers
- written permission from parents or carers will be obtained before photographs of pupils are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy
- learners' work can only be published with the permission of the learner and parents/carers.

## Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website [www.fountainsprimaryschool.co.uk](http://www.fountainsprimaryschool.co.uk)
- Social media
- Online newsletters
- Teachers2Parents Text Message Service

The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published without paren/carer consent.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use policies; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

The website includes an online reporting process for parents and the wider community to register issues directly to CEOP or SWGFL.

## Data Protection

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

The school:

- Esteem Multi-Academy Trust has a Data Protection Policy available at [www.esteemmat.co.uk/gdpr](http://www.esteemmat.co.uk/gdpr)
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- Esteem MAT has an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities', which is data mapping and highlights exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities (data maps) lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly [what personal data is held](#), where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- has procedures in place to deal with the individual rights of the data subject
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach as required by 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

- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff 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 will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software
- data will 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 and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices. [Procedures should be in place to enable staff to work from home \(i.e. VPN access to the school network, or a work laptop provided\).](#)
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

## Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, pupils; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors

- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice, and guidance have contributed to the development of this school Online Safety Policy template and of the 360 safe online safety self-review tool:

Copyright of these policy templates is held by SWGfL. Schools and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL ([onlinesafety@swgfl.org.uk](mailto:onlinesafety@swgfl.org.uk)) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in September 2022. However, SWGfL cannot guarantee it's accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2022