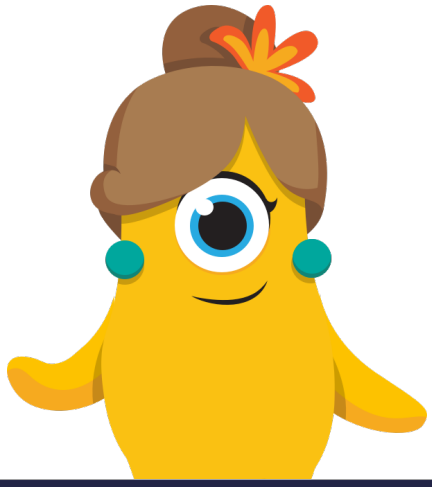


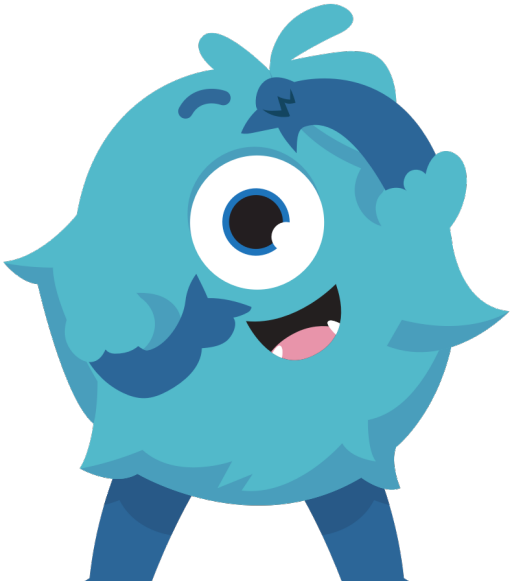
Florence Melly Community Primary School

Online Safety Policy

IF YOU CAN DREAM IT, YOU CAN DO IT!

Policy Approval

Policy Title:	Online Safety					**Date written:**		June 2024	
Written by:	Aaron Leach (Headteacher)					**New or revised policy:**		Revised	
Stakeholders consulted in policy production: (✓or x)	**Governors**	**SLT**	**Teaching Staff**	**Support Staff**	**Admin Staff**	**Parent/ Carers**	**Pupils**	**Local Community**	**External Agencies**
	✓	✓	✓	✓	✓	✓	✓	✓	✓
Implementation:	**Date of ratification:**			**Date presented to staff:**			**Date of renewal:**		
	8th July 2024			9th July 2024			July 2025		
Published on: (✓or x)	**School Website**			**School Prospectus/Induction Materials**			**Staff Handbook**		
	✓			✓			✓		



Florence Melly Community Primary School

Online Safety Policy - June 2024

Florence Melly Community Primary School is committed to safeguarding children and promoting children's welfare and expects all staff, governors, volunteers and visitors to share this commitment and maintain a vigilant and safe environment. Everyone has a responsibility to act, without delay, to protect children by reporting anything that might suggest a child is being abused or neglected. It is our willingness to work safely and challenge inappropriate behaviours that underpins this commitment. The school seeks to work in partnership with families and other agencies to improve the outcomes for children who are vulnerable or in need.

At Florence Melly Community Primary School we strongly believe that:

'Safeguarding and promoting the welfare of children is everyone's responsibility. Everyone who comes into contact with children and their families and carers has a role to play. In order to fulfil this responsibility effectively, all professionals should make sure their approach is child-centred. This means that they should consider, at all times, what is in the best interests of the child.' (DFE 2023)

Introduction

It is essential that our children are safeguarded from potentially harmful and inappropriate online material. Our school implements a whole school approach to online safety that sets out to protect and educate both children and staff in their use of digital technologies alongside establishing mechanisms to identify, intervene in and escalate any concerns, recognising that many children and young people have unlimited and unrestricted access to the internet via mobile phone and other digital devices.

Scope of the Online Safety Policy

This Online Safety Policy outlines our commitment to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) 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).

Policy development, monitoring and review

This Online Safety Policy has been developed by our Online Safety Working Group made up of:

- The Headteacher and/or senior leaders
- The Designated Safeguarding Lead (DSL)
- Our Computing Subject Leader
- Staff representatives
- Our Link Online Safety Governor/other Governors
- Parents/carers
- Representatives from our Junior Leadership Team

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

Schedule for development, monitoring and review:

This Online Safety Policy was approved by the *school governing body on:*	*8th July 2024*
The implementation of this Online Safety Policy will be monitored by:	*Headteacher/DSL*
Monitoring will take place at regular intervals:	*Termly*
The G*overning 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:	*Termly (through the Headteacher's Report to the FGB or the DSL's Report to the FGB).*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*July 2025*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*SIL safeguarding officer, police, Children's Services*

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents, collated on the school's CPOMS system
- Filtering and monitoring logs and reports
- Internal monitoring data
- Surveys/questionnaires capturing the voice of all stakeholders

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 our school.

Headteacher and Senior Leaders

- The Headteacher has 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 is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.

- 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.
- The Headteacher/Senior Leaders are responsible for ensuring that the Designated Safeguarding Lead/Online Safety Lead, IT provider/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.
- The Headteacher/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.
- The Headteacher/Senior Leaders will receive regular monitoring reports from the Designated Safeguarding Lead/Online Safety Lead.
- The Headteacher/Senior Leaders will work with the Link Governor, the Designated Safeguarding Lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the Link Online Safety Governor, who will receive regular information about online safety incidents and monitoring reports and report back to the FGB. The role of Online Safety Governor will include:

- Regular meetings with the Designated Safeguarding Lead/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)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the Link Governor) in-line with the DfE Filtering and Monitoring Standards
- Reporting to the FGB
- Receiving (at least) basic cyber-security training to enable the Governors to check that the school meets the DfE Cyber-Security Standards
- Membership of the school Online Safety Working Group

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

Designated Safeguarding Lead (DSL)

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 Link Online Safety Governor 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 Headteacher/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)
- Lead the Online Safety Working Group
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- Have a leading role in establishing and reviewing the school online safety policies/ documents/curriculum plans
- Promote an awareness of and commitment to online safety education/awareness raising across the school and beyond
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- 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
- Provide (or identify sources of) training and advice for all stakeholders
- Liaise with (school/local authority/external provider) technical staff, pastoral staff and support staff (as relevant)
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined in Keeping Children Safe in Education:

    - content
    - contact
    - conduct
    - commerce

Curriculum/Subject Leaders

Curriculum Leads will work with the DSL to develop and deliver a planned and coordinated online safety education programme.

This will be provided through:

- a discrete programme

- our RSHE programme
- cross-curricular programme linked to our Computing curriculum offer
- assemblies, national initiatives and celebrations (e.g. Safer Internet Day, Celebrating Social Media Day and Anti-Bullying Week), enrichment trips, visits and workshops and pastoral programmes.

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 acceptable use agreement and/or staff code of conduct
- they immediately report any suspected misuse or problem to the DSL or Senior Leadership Team for investigation/action, in line with the school's safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements
- 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 are guided to sites checked as suitable for their use and that procedures 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, there is regard to national safeguarding guidance and local safeguarding policies
- reinforce the school's 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.

IT Provider

The DfE Filtering and Monitoring Standards says:

"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider should work with the Senior Leadership Team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

Our school uses a technology service provided by an outside contractor (MGL). We work in collaboration to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. MGL follows and implements our school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from the local authority or other relevant body(ies)
- there is clear, safe, and managed control of user access to networks and devices
- 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
- the use of technology is regularly and effectively monitored in order that any misuse/ attempted misuse can be reported to the Headteacher/Senior Leaders or DSL for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring systems are implemented and regularly updated as agreed in school policies

Pupils

Are responsible for:

- using the school's digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- should 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.
- 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 and carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

Our school will take every opportunity to help parents/carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school, in accordance with our parent/carer code of conduct

- seeking their permissions concerning digital images, cloud services through our Universal Consent Forms
- parents'/carers' evenings, newsletters, 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.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

Community users/Visitors

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

Our school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

Online Safety Group

Our 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.

The Online Safety Group has the following members:

- The Headteacher and/or senior leaders
- The Designated Safeguarding Lead (DSL)
- Our Computing Subject Leader
- Staff representatives
- Our Link Online Safety Governor/other Governors
- Parents/carers
- Representatives from our Junior Leadership Team

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

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy and 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.

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". This is the case at

Florence Melly Community Primary School. Further details can be found on pages 33-34 of our policy. This can be accessed by clicking the following link: https://florencemelly.org/about-us/safeguarding/.

Our 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 through normal communication channels
- is published on the school website.

Acceptable Use

The school has defined what it regards as acceptable/unacceptable use through its acceptable use agreements. An acceptable use agreement is a document that outlines a school's expectations on the responsible use of technology by its users.

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.

Reporting and Responding

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. Our school also uses an online/anonymous reporting system, which can be accessed by all members of the school community via the school website. This is called SWGfL Whisper.

- 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 and other responsible staff have the 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, this may include:

    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy

- 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
- 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
        - 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 the school's CPOMS platform

- 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 (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:

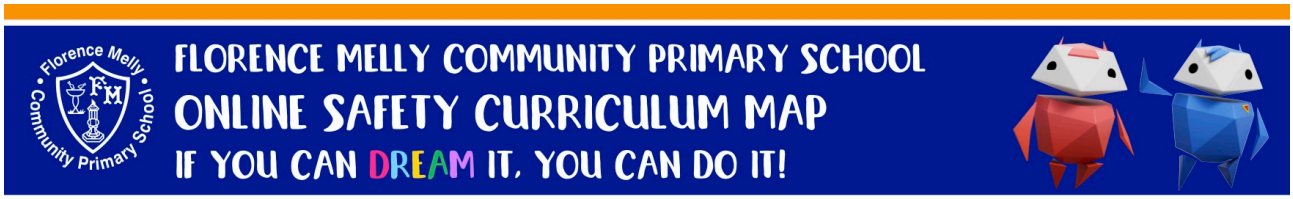
    - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - staff, through regular briefings
    - learners, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant

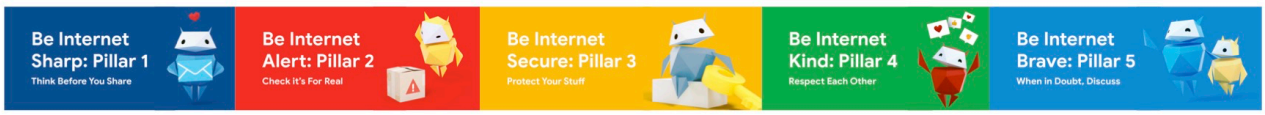
- The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

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. The school will actively seek advice from the Local Authority, SIL Safeguarding Team and the Police in more serious instances.

Online Safety Curriculum





Online Safety Long-Term Sequence Content Progression with our BIG IDEAS/PILLARS (Substantive Concepts)

Term	EYFS	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
Autumn	**Personal, Social and Emotional Development** **Self-Regulation ELG** Show an understanding of their own feelings and those of others, and begin to regulate their behaviour accordingly; Set and work towards simple goals, being able to wait for what they want and control their immediate impulses when appropriate. **Managing Self ELG** Be confident to try new activities and show independence, resilience and perseverance in the face of challenge; Explain the reasons for rules, know right from wrong and try to behave accordingly. **Building Relationships ELG** Show sensitivity to their own and to others' needs. **Childnet Smartie the Penguin** Seeing upsetting content, unreliable information, and being asked for personal information. Adverts, searching online, and online bullying.	**Childnet Smartie the Penguin** Upsetting or frightening content, pop-ups, and screen time.	**Childnet Smartie the Penguin** Downloading apps, fact versus opinion, and being asked to meet	**Be Internet Sharp/ Be Internet Alert** Online Reputations	**Be Internet Sharp/ Be Internet Alert** Opinions and Differences	**Be Internet Sharp** Positive Digital Footprints	**Be Internet Secure** Sharing, Settings and Passwords
Spring		**Childnet Smartie the Penguin** Contact from strangers, inappropriate games, and being asked for personal information.	**Childnet Smartie the Penguin** Screentime, password sharing, and online bullying.	**Be Internet Secure/ Be Internet Kind** Passwords and Behaviours	**Be Internet Secure/ Be Internet Kind** Making Good Decisions Online	**Be Internet Alert** Spotting Fake Information Online	**Be Internet Kind** Relationships and Being Kind
Summer		**Childnet Digiduck Stories** Being a good friend to others on the internet Understanding that what is read or seen online might be true, untrue, or someone's opinion. Playing games online, including peer pressure, password sharing, and in-app purchasing. Positive uses of the internet to help others	**NSPCC Techosaurus** Play and be kind online Protect your personal information Ask before you try something new online Say if anything has made you feel upset	**Be Internet Brave** Being Brave Online **Digital Wellbeing** How our screen use can affect the way we feel – both positively and negatively	**Be Internet Brave** Speak Up and Report It! **Digital Wellbeing** The mental and physical impact certain screen habits can have on us all and creating healthy digital habits	**Be Internet Brave** Refusing and Reporting **Digital Wellbeing** How our screen use can affect our Digital Wellbeing and reflect on how technology plays a role.	**Be Internet Brave** Handling and Reporting Mean Behaviour **Digital Wellbeing** The tools and knowledge that can be used to help enhance our Digital Wellbeing by creating our own healthy digital habits and making choices that work for us.

Our Online safety curriculum falls under our Cultural Capital Curriculum offer. However, it is a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. Our online safety curriculum is broad, relevant and provides progression. For more information about our curriculum offer, please use the following link: https://florencemelly.org/parents/online-safety/. We use the Google 'Be Internet Legends programme as a starting point: https://beinternetlegends.withgoogle.com/en_uk.

At Florence Melly Community Primary School, our online safety curriculum ensures: https://florencemelly.org/parents/online-safety/

- A planned curriculum offer for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve 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
- Learner need 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. Computing and RSHE; it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day, Celebrating Social Media Day and Anti-Bullying Week, enrichment trips, visits and workshops and pastoral programmes.
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- learners are helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.
- staff 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, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff are 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
- our online safety education programme is relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Pupils

Our school acknowledges, learns from, and uses the skills and knowledge of learners 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 learner feedback and opinion like regular surveys and Pupil Book Study

- the appointment of digital leaders/anti-bullying ambassadors/junior leadership team members and other advocacy roles
- the Online Safety Group has learner representation
- learners designing/updating acceptable use agreements
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes 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 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 and data protection training will be made available to all staff. 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.
- 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 (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- the Designated Safeguarding Lead/Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required, through our e-bulletin system
- resources made available to staff through an online safety noticeboard located in the staffroom

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 several ways such as:

- attendance at training provided by the local authority/MAT or other relevant organisation
- participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).
- e-bulletin updates posted to Governorhub

A higher level of training will be made available to (at least) the Online Safety LinkGovernor. This will include:

- cyber-security training (at least at a basic level)
- training to allow the Link Governor to understand the school's filtering and monitoring provision, so that they can effectively carry out the required checks, review and scrutinise reports.

Families

Many parents/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/carers 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.

To address this, our school will seek to provide information and awareness to parents/carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops/parent/carer evenings etc
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings
- letters, newsletters, website, posts on Class Dojo
- high profile events / campaigns e.g. Safer Internet Day

Adults and Agencies

Our school will provide opportunities for local community groups and members of the wider community to benefit from our school's online safety knowledge, experience and expertise. 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
- providing online safety information via our website and social media for the wider community
- supporting community groups.

Technology

The school is 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. We are supported with this by our MGL, our IT provider. We ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:

"It is essential that governing bodies and proprietors ensure that appropriate filtering 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 filtering 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 appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

The school filtering and monitoring provision is agreed by Senior Leaders, Governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

Checks on the filtering and monitoring system are carried out by the with the Designated Safeguarding Lead/Headteacher and a Governor (where possible) with the support of our IT Service Provider, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access, BYOD or new technology is introduced.

Filtering

Our school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.

Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL 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, recognising that no system can be 100% effective.

There is a clear process in place to deal with, and log, requests/approvals for filtering changes.

Filtering logs are regularly reviewed and alert the Headteacher and Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.

The school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)

Younger learners will use child friendly/age-appropriate search engines e.g. https://swiggle.org.uk/

The school has a mobile phone policy and no personal mobile devices have internet access through the school network.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users.

The school monitors all network use across all its devices and services.

Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Headteacher or Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.

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.

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 informed by the school's risk assessment. These may include:

- physical monitoring (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
- Use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s). This is called Smoothwall.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- responsibility for technical security resides with the Headteacher and SLT who may delegate activities to identified roles
- 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 service provider and will be reviewed, at least annually, by the SLT/Online Safety Group
- password procedures are encouraged and implemented (consistent with guidance from the National Cyber Security Centre)
- all users 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.
- servers, wireless systems and cabling are securely located and physical access restricted
- 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 by our IT provider. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud
- the Headteacher is responsible for ensuring that all software purchased by and used by the school is adequately licensed and that the latest software updates (patches) are applied
- an appropriate system is in place for users to report any actual/potential technical incident/ security breach to the relevant person, as agreed
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is prohibited

- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit
- guest users/visitors are provided with appropriate access to school systems based on an identified risk profile.

Mobile technologies

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

The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device	Pupil owned	Staff owned	Visitor owned
Allowed in school	✔	✔	✔	✔ (in Year 6)	✔	✔
Full network access	✔	✔	✔	-	-	-
Internet only	-	-	-	-	-	-
No network access	-	-	-	✔	✔	✔

School owned/provided devices:

- all school devices are managed though the use of Mobile Device Management software
- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- guidance is in place to support responsible use.

Personal devices:

- there is a clear policy covering the use of personal mobile devices on school premises for all users
- where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage is made available (please see our mobile phone policy for further details)
- use of personal devices for school business is defined in the acceptable use agreements.
- the expectations for taking/storing/using images/video aligns with the school's acceptable use agreement/staff code of conduct
- there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements
- education about the safe and responsible use of mobile devices is included in the school online safety education programmes

Social media

With widespread use 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 include the protection of learners, the school and the individual when publishing any material online.

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. This is reinforced and communicated through the school's code of conduct for adults.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff.

The 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 pupils, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

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

- clear processes for the administration, moderation, and monitoring of these accounts
- a code of conduct/policy 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.

Social Media - 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 school hours

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.

Our school will 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 Designated Safeguarding 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 learners 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.

Our school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

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.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* 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, storage, distribution and publication of those images

Care should be taken when sharing digital/video images that pupils are appropriately dressed.

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 this Online Safety Policy.

Pupils' full names will not be used, by the school, anywhere on a website or Class Dojo, particularly in association with photographs.

Written permission from parents/carers will be obtained before photographs of pupils are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes.

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

Online Publishing

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

- Public-facing website
- Social media platforms
- Online newsletters
- Class Dojo

The school website is managed by Clarity Creation and hosted by 34SP.com.

The school ensures that this 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 pupil work, images or videos are published, their identities are protected, and full names are not published.

Our website includes an online reporting process for parents/carers and the wider community to register issues and concerns to complement the internal reporting process.

Data Protection

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

Our school:

- has a Data Protection policy
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest
- 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
- 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/carers to check emergency contact details at suitable intervals
- provides staff, parents/carers and volunteers 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, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- 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
- 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 72 hours 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 the Local Authority to help ensure the development of a consistent and effective local online safety strategy.