Policy
Online Safety

This policy has been written with regard to the guidance 'Working together to safeguard children', 'Keeping children safe in education' and the 'Special Education Needs Code of Practice', which places Special Education Needs and Disabilities together and abbreviated to SEND. A copy can be seen in the Headteacher's Office.

The overall objective of the school's Equality Policy, in line with the Equality Act 2010, is to provide a framework for the school to pursue its equality duties to eliminate unlawful discrimination and harassment, promote equality of opportunity, and promote good relations and positive attitudes between people of diverse backgrounds in all its activities.

Title	Online Safety Policy
Date of Issue	October 2023
Review Date	September 2024
Prepared by	Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL)
To be reviewed by	Headteacher and Governors
Appendices	Appendix 1: Acceptable Use of Technologies Policy – YR and KS1 Appendix 2: Acceptable Use of Technologies Policy – KS2 Appendix 3: Acceptable Use of Technologies Policy – Parents/ Carers Appendix 4: Acceptable Use of Technologies Policy for staff Appendix 5: Acceptable Use of Technologies Policy for supply staff Appendix 6: Terms and Conditions for our guest WiFi (for visitors and volunteers) Appendix 7: Reporting System for Online Safety – flowchart Appendix 8: Photograph and Name Consent Form
Supply / distribution	Available as a read-only document on the Fynamore school website and a hardcopy in the school office.
Other relevant approved documents	Child Protection and Safeguarding Policy Behaviour Policy Staff Disciplinary Procedures Data Protection Policy and Privacy Notices Complaints Procedure Curriculum Policy including Computing Personal use of Social Media for Staff, Governors and Support Staff

Authorised by	Headteacher and Governors

Fynamore Primary School

Online Safety Policy

This policy applies to all members of the school community (including staff, learners, 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).

Date created: October 2023

Next review date: September 2024

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Fynamore Primary School 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).

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

Policy development, monitoring and review

This Online Safety Policy has been developed by the

- Designated Safeguarding Lead (DSL) – Kate Hurst
- Online Safety Lead (OSL) – Alan McArtney
- Staff – including technical staff

Schedule for development, monitoring and review

This Online Safety Policy was approved by the *school governing body on:*	
The implementation of this Online Safety Policy will be monitored by:	*The Designated Safeguarding Lead (Kate Hurst) and Online Safety Lead (Alan McArtney)*
Monitoring will take place at regular intervals:	*Annually*
The *governing body* will receive a report on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents) at regular intervals:	*3 X per year in Headteacher's report to Governors.*
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:	*September 2024*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*MASH* *Police*

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- Analysis of reported online safety incidents on CPOMS.
- Filtering and monitoring logs
- Internal monitoring data for network activity
- Online Safety surveys

Policy and leadership

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.

The Headteacher:

- 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 2023.
- The Headteacher and the DSL 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 is responsible for ensuring that the Designated Safeguarding Lead, Online Safety Lead, Oakford 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 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 receive regular monitoring reports from the Designated Safeguarding Lead.
- The Headteacher will work with the Nominated Governor (Jacqui Radford), the Designated Safeguarding Lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors

The DfE guidance "Keeping Children Safe in Education 2023" 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"
>
> "Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of Designated Safeguarding Lead. The DSL should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

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 Nominated Online Safety Governor (Jacqui Radford) who will receive regular information about online safety incidents and monitoring reports.

The role of Online Safety Governor will include:

- regular meetings with the Designated Safeguarding Lead and Online Safety Lead
- regularly receive (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 the DSL and Oakford (IT Provider) and involve the Nominated Governor) - in-line with the DfE Filtering and Monitoring Standards (Keeping Children Safe in Education 2023).
- sharing information in relevant *Governors meeting*s
- receiving basic cyber-security training to ensure that the school meets the DfE Cyber-Security Standards

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

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"

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
- 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
- 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.
- meet regularly with the Nominated Online Safety Governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual filtering and monitoring checks are carried out
- report regularly to the Headteacher
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

The Online Safety Lead will work closely with the DSL. Furthermore they will:

- 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
- promote an awareness of and commitment to online safety education/ awareness raising across the school and beyond
- liaise with the curriculum leader to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with Oakford 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

The Computing Lead will:

- work with the DSL and OSL to develop a planned and coordinated online safety education programme through Purple Mash.

This will be provided through:

- a discrete Computing scheme of work (Purple Mash)
- our Personal Development curriculum, including SCARF.
- a mapped cross-curricular programme
- assemblies and events such as 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 /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 Policy (AUP)
- they immediately report any suspected misuse or problem to *the Designated Safeguarding Lead (Kate Hurst)* for investigation/action, in line with the school 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 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 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 processes are in place for dealing with any unsuitable material that is found in internet searches*
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment and discrimination
- 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.

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."*
>
> Our IT service provider (Oakford) will have technical responsibility for:
>
> - maintaining filtering and monitoring systems
> - providing filtering and monitoring reports
> - completing actions following concerns or checks to systems
>
> Our IT service provider (Oakford) will work with DSL to:
>
> - procure systems
> - identify risk
> - carry out reviews
> - carry out checks

Our IT service provider (Oakford) is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and procedures 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 Wiltshire Council.
- 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 DSL (Kate Hurst) for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is the responsibility of Oakford.
- *monitoring systems are implemented and regularly updated as agreed in school policies*

Our pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy 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 and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the Pupils Acceptable Use Policy
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images etc.
- parents'/carers' evenings, newsletters, website, social media and information about national/ local online safety updates.

Parents and carers will be encouraged to support the school in reinforcing the online safety messages provided to children in school.

Community users

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

The 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.

Professional Standards

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 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
- is published on the school website.

Acceptable Use Policies

The Acceptable Use Policies define acceptable use at the school. These will be communicated and re-enforced through:

- pupil home/ school agreement
- staff induction pack
- posters in classrooms
- communication with parents/carers
- built into education sessions
- school website

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 the Headteacher (Sarah Weber) – 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:

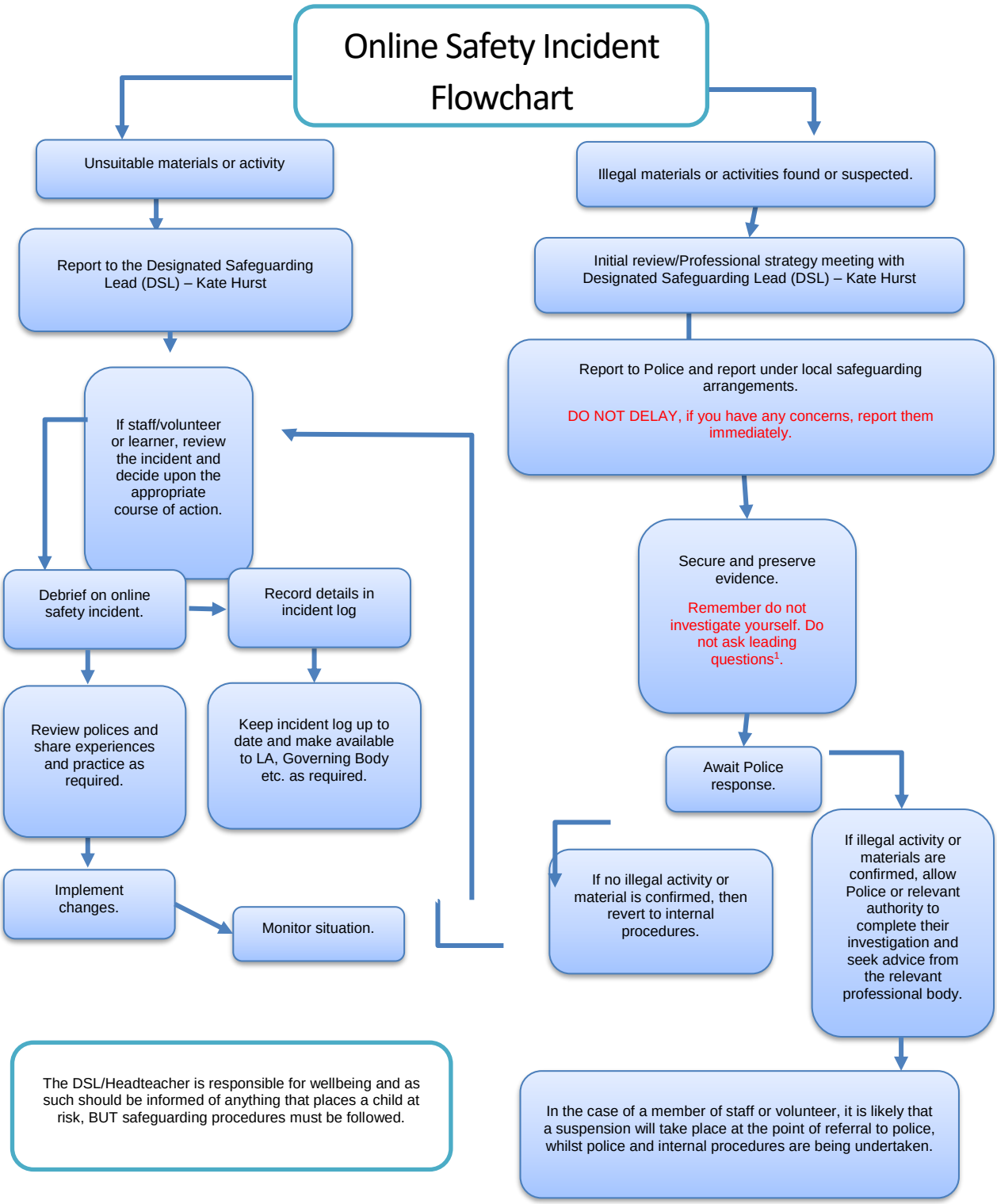
> *"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual 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 in a timely manner
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead and Online Safety Lead 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 (see flowchart and user actions chart on page 11), 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 (Robert Parker) and the DOfA.
- 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 will be recorded
- 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 staff meetings
    - pupils, through assemblies/lessons
- parents/carers, through newsletters, school social media, website
- governors, through regular safeguarding updates
- Wiltshire Council and 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.


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) – Kate Hurst
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL) – Kate Hurst
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

It is more likely that Fynamore Primary 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 procedure.

Online Safety Curriculum

The Online Safety Curriculum an essential part of the school's online safety provision. Pupils need help and support 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'.."*

Keeping Children Safe in Education states:

> "*Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum …"*

Online safety 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, with opportunities for creative activities.

Our curriculum will be provided in the following ways:

- A planned online safety curriculum taught through Purple Mash which is matched to Education for a Connected World.
- 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 taught through other curriculum areas e.g. Personal Development.
- 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 pupils at different ages and abilities such as those with SEND or vulnerable children.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Policy aand encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum.
- 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 pupils and monitoring the content of the websites that pupils visit.

- it is accepted that from time to time, for good educational reasons, students may need to research topics or have access to resources, 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

Contribution of pupils

The 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:

- pupil feedback
- appointment of Online Safety Leaders
- pupils contribute to the online safety education programme e.g. leading lessons for younger learners, contributing towards assemblies and online safety campaigns
- pupils designing/ updating acceptable use agreements
- contributing to online safety events with the wider school community e.g. parent/ carer information evenings

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

- the training will be an integral part of the school's annual safeguarding and child 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 policies.
- the Online Safety Lead and Designated Safeguarding Lead will receive regular updates and training.
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings/ TD days
- the Designated Safeguarding Lead/ Online Safety Lead will provide advice/guidance/training to individuals as required.

Governors

Governors will take part in annual online safety training delivered by the DSL.

The Nominated Governor for online safety will take part in:

- Cyber-security training
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

Families

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

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

- sharing Acceptable Use of Technologies Policies for parents and pupils.
- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- opportunities for engagement with parents and carers on online safety issues through awareness workshops.
- newsletters, website, social media
- high profile events / campaigns e.g. Safer Internet Day

Technology

Fynamore Primary School is responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. We will 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 SLT, Governors and the IT Service Provider (Oakford) 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 IT Service Provider with the involvement of a the Designated Safeguarding Lead and the Nominated Governor for Online Safety, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access, BYOD (Bring Your Own Device) or new technology is introduced.

Filtering

- the 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 (see Appendix for more details).
- filtering logs are regularly reviewed and alert the 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.)*
- *the school has a mobile phone policy and 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 Oakford IT Services.

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.
- Weekly monitoring reports sent by Oakford are picked up, acted on and outcomes are recorded by the 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*
- *We have sought advice from Oakford and are carefully considering the use of a third-party assisted monitoring service to review monitoring logs and report issues to the DSL and OSL. Securus Solutions has been recommended.*

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 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 policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- the security of their username and password and must not allow other users to access the systems using their log on details.
- 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.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- there is a risk-based approach to the allocation of learner usernames and passwords
- 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
- appropriate security measures are in 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 software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- Jen Maitland (Business Manager) is responsible for ensuring that all software purchased by and used by the school is adequately licensed and that the latest software updates 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 regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/ Oakford
- removable media is not permitted unless approved by the SLT/ Oakford
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place
- guest users are provided with appropriate access to school systems based on an identified risk profile.

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 provided or personally owned and might include smartphone, tablet, wearable devices, 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 learning platform and other cloud-based services such as e-mail and data storage.

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

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

School 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
- any designated mobile-free zone is clearly signposted
- personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
- liability for damage aligns with current school policy for the replacement of equipment.
- education 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 devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.
- use of personal devices for school is defined in the acceptable use policy. Personal devices commissioned onto the school network are segregated effectively from school-owned systems
- the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- liability for loss/damage or malfunction of personal devices is clearly defined
- 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 this policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages will 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.

All schools have a duty of care to provide a safe learning environment for learners 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.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- guidance is 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 children and 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 used, there will 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 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.
- 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 learners instant use of images that they have recorded themselves or downloaded from the Internet. However, staff, parents/carers and children need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out Internet searches for information about potential and existing employees.

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

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance/ policies?
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.

- staff/ volunteers must be aware of those children 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 learners are appropriately dressed
- photographs published on the website, or elsewhere that include children will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners 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
- images will be securely stored in line with the school retention policy
- Children's work can only be published with the permission of the child and the parent/carer.

Online Publishing

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

- Our school website
- Social media
- Online newsletters

The school website is managed/ hosted by Wix. Sophie Croxford (office admin) regularly checks and updates the school website.

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 children's work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use policy; 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 and concerns to complement the internal reporting process.

Outcomes

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

- there is balanced discussion about the evidence taken from the 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 the above.

Appendix 1 – Acceptable Use of Technologies Policy – YR and KS1

Fynamore Primary School

Acceptable Use of Technologies Policy for Pupils – YR and KS1

This is how we stay safe when we use laptops, iPads and other devices in school:

- I will ask a teacher or another adult in school if I want to use the laptops or iPads.
- I will only use laptops and iPads for activities that a teacher or adult has told or allowed me to use.
- I will take care of the laptops, iPads and other equipment.
- I will ask for help from a teacher or another adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or another adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use the laptop or iPad.

Appendix 2: Acceptable Use of Technologies Policy – KS2

Fynamore Primary School

Acceptable Use of Technologies Policy for Pupils – KS2

I understand that I must use school laptops, iPads and the Internet in a responsible way, to ensure that there is no risk to my safety or to the safety of others.

For my own safety:

- I understand that the schools will monitor my use of the school devices (laptops and iPads) and systems.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down a password as someone may steal it.
- I will be aware of "stranger danger", when I am communicating online.
- I will not share personal information about myself or others when online (this could include names, home addresses, email addresses, telephone numbers, age, my school details)
- I will report any unkind or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online straight away.

I understand that everyone has the right to use technology:

- I understand that the school's devices and Internet are for educational use and that I will not use them for personal use unless I have permission.
- I will not try to make large downloads or uploads that might take up the capacity of the Internet and stop other children from being able to do their work.
- I will not use the school's Internet or devices for online gaming, online gambling, Internet shopping or video broadcasting (e.g. YouTube).

I will act as I expect others to act towards me:

- I will respect others' work and will not access, copy, remove or change any computer files that belong to somebody else.
- I will be polite and responsible when I communicate with others
- I will not use unkind or inappropriate language and I appreciate that others may have different opinions to my own.
- I will not take or share images of adults or children in school without their permission.

I understand that the school has security and safety rules:

- If I bring my own personal device into school (e.g. a mobile phone or tablet) then I will make sure this is handed in to the office at the beginning of the school day or handed to my class teacher to be locked in the classroom cupboard.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- I will not use any programmes that might allow me to bypass the filtering/ security systems in place to prevent access to inappropriate materials.
- I will immediately report any damage or faults involving laptops or iPads, however this may have happened.
- I will not open any attachments in emails, unless I know and trust the person who sent the email.
- I will not install or attempt to install or store programmes of any type on a school laptop or iPad
- I will not alter the computer settings

When using the Internet, I know that:

- When I am using the Internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful.
- Where work is protected by copyright, I will not try to download copies (including music and videos)

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school has a responsibility to follow up any incidents of inappropriate online behaviour when I am out of school such as online-bullying, inappropriate use of images or personal information.
- I understand that if I do not follow this Acceptable Use Policy then I may lose access to school laptops, iPads and the Internet. I may also receive a behaviour consequence and my parents/ carers may be contacted. In the event of illegal activities, we may need to involve of the police.

Appendix 3: Acceptable Use of Technologies Policy – Parents/ Carers

Fynamore Primary School

Acceptable Use of Technologies Policy for Parents/ Carers

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

This acceptable use policy is intended to ensure that:

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

The school will aim to ensure that children have good access to digital technologies to enhance their learning and will, in return, expect the children to agree to be responsible users.

As a parent/carer:

- I will give permission for my child to have access to the digital technologies at school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the Internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet and using mobile technologies.
- I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.
- I will encourage my child to adopt safe use of the internet and digital technologies at home (e.g. by applying parental locks) and will inform the school if I have concerns over my child's online safety.

Use of Digital/ Video Images

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

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

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

In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos and digital images of their children at school events for their own personal use. 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.

Appendix 4: Acceptable Use of Technologies Policy for staff

Fynamore Primary School

Acceptable Use of Technologies Policy for Staff

School Policy

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

This acceptable use policy is intended to ensure that:

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

Fynamore Primary School will aim to ensure that staff have good access to digital technology to enhance their work and to enhance learning opportunities and will, in return, expect staff to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate children in my care in the safe use of digital technology and embed online safety in my work with children.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I will not use my personal devices such as my mobile phone, my personal laptop or my tablet through the school network.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, iPad, email) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the DSL and/ or Headteacher (Kate Hurst and/ or Sarah Weber).

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of children I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website/ Social Media) it will not be possible to identify by full name, or other personal information, those who are featured.
- I will only communicate with children and parents/carers using Seesaw. Any such communication will be professional in tone and manner. Admin staff will use ParentMail and school office email to communicate with parents/ carers.
- I will not engage in any online activity that may compromise my professional responsibilities.

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

- I will not access personal email or personal Social Media accounts on the school's IT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography) or inappropriate or may cause harm or distress to others.
- I will not use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer. All requests must go through our IT Provider (Oakford)
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: ----------

Signed: ----------

Date: ----------

Appendix 5: Acceptable Use of Technologies Policy for supply staff

Fynamore Primary School

Acceptable Use of Technologies Policy for Supply Staff

To be completed once per year and in the event of a new supply teacher working at Fynamore.

Fynamore Primary School will aim to ensure that supply staff have access to digital technology to enhance their work and to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate children in my care in the safe use of digital technology and embed online safety in my work with children.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I will not use my personal devices such as my mobile phone, my personal laptop or my tablet through the school network.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, iPad, email) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set by the school.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the DSL and/ or Headteacher (Kate Hurst and/ or Sarah Weber).

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website/ Social Media) it will not be possible to identify by full name, or other personal information, those who are featured.
- I will not engage in any online activity that may compromise my professional responsibilities.

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

- I will not access personal email or personal Social Media accounts on the school's IT systems.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography) or inappropriate or may cause harm or distress to others.
- I will not use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the school digital technology systems in school within these guidelines.

Name: ----------

Signed: ----------

Date: ----------

Appendix 6: Terms and Conditions for our guest WiFi (for visitors and volunteers)

Guest WiFi Terms and Conditions

Please read the following information carefully before using this service. You may not use the service without accepting these Terms and Conditions.

Welcome to the wireless high-speed Internet access system ("Guest Wifi System") at Fynamore School. These "Terms and Conditions of Use", govern your rights and responsibilities and our rights and responsibilities relating to the use of the Guest Wifi System at Fynamore School.

Acceptance of Terms and Conditions of Use

By continuing to the internet you are confirming that:

1. YOU HAVE READ, UNDERSTAND AND AGREE TO THE TERMS OF THIS AGREEMENT AND

2. YOU ARE AT LEAST 18 YEARS OF AGE.

If you do not agree to the terms of this Agreement, you may not use the school Guest Wifi System.

Description of Guest Wifi System/Service Availability

Fynamore School will provide access to the Guest Wifi System at locations ("Enabled Locations") that have been equipped with wireless access points. Access points or Enabled Locations may not be available in all areas of the school, and may not always be operational.

Access to Internet

Fynamore School does filter and restrict access to certain content placed on or accessible through the Internet. Fynamore School does not screen or restrict communications between parties via the Internet. You acknowledge that if you access the Internet you may receive or be exposed to content, goods or services which you consider to be improper, inaccurate, misleading, defamatory, obscene or otherwise offensive. You agree that Fynamore School is not liable for any action or inaction with respect to any such content on the Internet accessible through the Guest Wifi System.

Your Responsibilities

You must (1) provide all equipment (including computer hardware and software, personal digital assistants, wireless network cards, etc.) to connect to the Guest Wifi System, (2) comply with UK GOVERNMENT and international laws and regulations, including but not

limited to copyright and intellectual property rights laws. You agree to be responsible for and to bear all risk and consequences for (1) the accuracy, completeness, reliability and/or usefulness of any content available through the Guest Wifi System and (2) all communications that you send or receive via the Guest Wifi System. Fynamore School does not undertake the security of any data you send through the Guest Wifi System and it is your responsibility to secure such data.

Acceptable Use Policy

All users of the Guest Wifi System must comply with this Acceptable Use Policy (AUP). This AUP is intended to prevent unacceptable uses of the Internet. Fynamore School does actively monitor the use of the Guest Wifi System under normal circumstances. We may remove, block, filter or restrict by any other means any materials that, in our sole discretion, may be illegal, may subject Fynamore School to liability or may violate this AUP. Fynamore School may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong. Violation of this AUP may result in the suspension or termination of your access to the Guest Wifi System.

The following constitute examples of violations of this AUP.

You agree to not use the Guest Wifi System to:

(1) Transmit any material (by uploading, posting, email or otherwise) that is unlawful, threatening, abusive, harassing, tortious, defamatory, obscene, libelous, invasive of another's privacy, hateful or racially, ethnically or otherwise objectionable;

(2) Harm, or attempt to harm, minors in any way;

(3) Impersonate any person or entity or falsely state or otherwise misrepresent your affiliation with a person or entity; forge headers or otherwise manipulate identifiers in order to disguise the origin of any material transmitted through the Guest Wi-Fi System;

(4) Transmit any material (by uploading, posting, email or otherwise) that you do not have a right to make available under any law or under contractual or fiduciary relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under non-disclosure agreements);

(5) Transmit any material (by uploading, posting, email or otherwise) that infringes any patent, trademark, trade secret, copyright or other proprietary rights of any party;

(6) Transmit (by uploading, posting, email or otherwise) any unsolicited or unauthorised advertising, promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes" or any other form of solicitation;

(7) Transmit any material (by uploading, posting, email or otherwise) that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;

(8) Interfere with or disrupt the Service or servers or networks connected to the Service, or disobey any requirements, procedures, policies or regulations of networks connected to the Service;

(9) Intentionally or unintentionally violate any applicable local, national or international law, or any regulations having the force of law;

(10) "Stalk" or otherwise harass another; or collect or store, or attempt to collect or store, personal data about third parties without their knowledge or consent;

(11) Resell the Guest Wifi System.

(12) Use the Guest Wifi System for high volume data transfers, especially sustained high volume data transfers, hosting a web server, IRC server, or any other server.

You understand and agree that Fynamore School may disclose your communications and activities using the Guest Wifi System in response to lawful requests by governmental authorities and judicial orders.

Fynamore School requests that anyone who believes that there is a violation of this AUP direct the information to office@fynamore.org.uk and include "GUEST WIFI" in the subject line. If available, please provide the following information:

(1) the IP address used to commit the alleged violation;

(2) the date and time of the alleged violation, including the time zone;

(3) evidence of the alleged violation; and

(4) your contact details including full name, email address and telephone number.

When reporting an issue regarding unsolicited email please provide a copy of the email messages with full headers which typically provides all of the above data. Other situations will require different methods of providing the necessary information.

Termination

You agree that Fynamore School may terminate this Agreement and cancel your access to the Guest Wifi System at any time, without notice and for any reason including, but not limited to, violation of any of the terms and conditions of this Agreement, security or safety

reasons, and/or using the Guest Wifi System to perform any illegal activity. You further agree that in the event of termination for any reason, Fynamore School will have no liability to you.

Modifications

Fynamore School may, at its sole discretion, modify the terms and conditions of this Agreement, including the AUP, at any time. Such modifications shall be binding and effective upon posting on the Guest Wifi System 'Internet Access Signup' page. You agree to periodically review the 'Internet Access Signup' page to maintain awareness of any modifications. By continuing to use the Guest Wifi System after such postings, you accept and agree to any and all such modifications.

Indemnification

You shall defend, indemnify and hold Fynamore School and its corporate affiliates and their respective officers, directors, employees, contractors, agents, successors and assigns harmless from and against, and shall promptly reimburse them for, any and all losses, claims, damages, settlements, costs, and liabilities of any nature whatsoever (including reasonable legal fees) to which any of them may become subject arising out of, based upon, as a result of, or in any way connected with, your use of the Guest Wifi System or any breach of this Agreement.

No Warranty

THE GUEST WIFI SYSTEM IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS, WITHOUT WARRANTIES OF ANY KIND. THE FYNAMORE SCHOOL DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS. FYNAMORE SCHOOL MAKES NO EXPRESS WARRANTIES AND CUSTOMER WAIVES ALL IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF TITLE, NON INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE REGARDING ANY MERCHANDISE, INFORMATION OR SERVICE PROVIDED THROUGH FYNAMORE SCHOOL OR THE INTERNET GENERALLY. CUSTOMER EXPRESSLY ACKNOWLEDGES THAT THERE ARE, AND ASSUMES ALL RESPONSIBILITY RELATED TO, THE SECURITY, PRIVACY AND CONFIDENTIALITY RISKS INHERENT IN WIRELESS COMMUNICATIONS AND TECHNOLOGY AND FYNAMORE SCHOOL DOES NOT MAKE ANY ASSURANCES OR WARRANTIES RELATING TO SUCH RISKS. NO ADVICE OR INFORMATION GIVEN BY FYNAMORE SCHOOL OR ITS REPRESENTATIVES SHALL CREATE A WARRANTY.

Limitation of Liability

FYNAMORE SCHOOL, ITS EMPLOYEES, AGENTS, VENDORS, AND LICENSORS ARE NOT LIABLE FOR ANY COSTS OR DAMAGES ARISING, EITHER DIRECTLY OR INDIRECTLY, FROM YOUR USE OF THE GUEST WIFI SYSTEM OR THE INTERNET,

Appendix 7: Reporting system for Online Safety – flowchart (child friendly)

Reporting System for Online Safety – Fynamore Primary School

You have an Online Safety issue or worry

↓

Tell a trusted adult in school or at home or you could speak to Childline.

ChildLine 0800 1111

↓

Fill out an Online Safety concern form.

An adult can help you to complete this.

↓

The form will be handed in to Mrs Hurst and she will decide if any further action is needed. She will also take steps to make sure that it doesn't happen again.

↓

The concern or issue may be discussed with parents and may involve the police.

Appendix 8: Photograph and Name Consent Form

Fynamore Primary School

Photograph & Name Consent Form

Please complete, sign and return to the school office.

All photographs/data will be collected, stored and used under the terms of our Privacy Notice and the GDPR Regulations

Pupil name:	***Class:***

Parent's Consent for Photographs in the Media, on Social Media and the school website

On occasion, the school may wish to publish photographs/video/sound files of children for the purpose of promoting, publicising or celebrating school activities and events or entering competitions. For example: media (such as printed newspapers, online newspapers), school media platform (such as Facebook, Instagram) and the school website.

Photograph & Name Consent *- Please tick <u>one</u> of the options below:*

- ☐ I agree to my child's photograph and full name.
- ☐ I agree to my child's photograph and first name.
- ☐ I agree to my child's unnamed photograph.
- ☐ I do not agree to my child's photograph.

On occasion, the school may wish to publish just a child's name in the media, on social media, on school website or in the school newsletter (which goes on the school website). For example, if they win 'Star of the Week', or a sporting or colouring competition, etc.

Name Consent Only *– Please tick <u>one</u> of the options below:*

- ☐ I agree to my child's full name being published.
- ☐ I agree to my child's first name being published.
- ☐ I do not agree to my child's name being published.

Parent's Consent for Photographs within the school setting eg: Seesaw, YR learning journeys

Photographs are often taken as part of our every day school life, to share experiences, celebrate work and to aid or evidence learning. Photographs might, for example, be used in learning journeys, on the Seesaw app, school displays, in class books or to share great news (such as 'Star of the Day' in YR, or 'Star of the Week'). These unnamed photographs may be of groups or individuals, depending on the learning taking place. They may be seen by other parents visiting the school or on the Seesaw app. Please be assured that these photos are never named, with the exception of your own child - in their own book/Seesaw/learning journey. These photographs are only shared in school and on Seesaw as part of our learning experience.

Photographs in school, on Seesaw or in learning journeys – *Please tick <u>one</u> of the options below:*

☐ I consent ☐ I do not consent

Parent's consent for Photographs taken by professionals eg: yearly photos, class photos

We also have professional photographers who come into school to take whole class, school and group photographs. Class photographs are offered for sale to parents and whole school photos are displayed in school. These photographs are never named.

Professional taken photographs – *Please tick <u>one</u> of the options below:*

☐ I agree ☐ I do not agree

Signed:	Date:
Please print name:	