Online Safety Policy

Deepdale Community Primary School

Updated October 2024

Contents

Online Safety Policy 2024/2025

Deepdale Community Primary School

Introduction

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Deepdale Community 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, pupils, parents/carers, governors, visitors, volunteers, and school community users) who have access to and are users of school digital systems, both in and out of school. It also applies to the use of personal digital technology on the school site.
Deepdale Community 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 an **online safety group** made up of:

- Head teacher/Designated Senior Leader for safeguarding (DSL)
- Computing subject leader
- Staff-including teachers, health and safety officer, computer IT Network Manager
- Governors
- Parents and Carers
- Community Users

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

Schedule for Development/Monitoring/Review

This online safety policy has been developed but makes close reference to and needs to be read in conjunction with other national guidelines and school policies:

- Revised *Prevent* Duty Guidance: for England and Wales-March 2024
- Keeping Children Safe in Education (September 2024)
- Teaching online safety in school (January 2023)
- Education for a connected World (June 2020)
- Online Radicalisation- guidance for Schools (August 2024)
- Lancashire County Council Whistleblowing Policy for all staff in Delegated Schools (April 2024)
- Deepdale Community Primary School Safeguarding and Child protection policy
- Deepdale Community Primary School Anti-Bullying policy
- Deepdale Community Primary School Health and Safety policy
- Deepdale Community Primary School SEND policy.
- Deepdale Community Primary School Data Protection policy
- Deepdale Community Primary School Freedom of Information policy
- Deepdale Community Primary School Computing policy
- Deepdale Community Primary School policy with regards to the use of Mobile Phones.
- Deepdale Remote Learning Plan

This online safety policy was approved by the Governing Body on:	
The implementation of this online safety policy will be monitored by the:	Head teacher/DSL, computing subject leaders, governor responsible for safeguarding and IT Network Manager.
The governing body will receive a report on the implementation of online safety generated by the monitoring group (which will include details of online safety incidents at regular intervals)	This will happen each term.
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	October 2025
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Lancashire online safety team Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys/questionnaires of pupils, parents/carers, staff
- Monitoring logs of internet activity
- Internal monitoring data for network activity

The policy will be communicated to staff/pupils/community in the following ways:

- The policy will be posted on the school website.
- The policy will form part of the pack for new members of staff.
- Regular updates and training about online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to school.

Policy and Leadership

Roles and 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. Whilst this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within school.

Role	Responsibility
Governing body/ Safeguarding governor	• Be responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. • This review will take place by providing the Safeguarding governor with information about online safety incidents and monitoring reports. • Regular reviews with the DSL to focus on online safeguarding in our school and feedback to governors' meetings. • Regularly receive (collated and anonymised) reports of online safety incidents • Checking 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.
Head teacher/DSL	• 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 (DSL), as defined in Keeping Children Safe in Education (KCSIE). • Be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. • Be responsible for ensuring that the deputy DSL, computing subject leaders, technical staff and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. • 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. • Will receive regular monitoring reports from the health and safety officer and IT Network Manager see filtering and monitoring policy.
Senior leaders/DSL's/Pastoral team	• Receive reports of online safety issues, begin aware of the potential for serious child protection concerns and ensuring that these are logged to inform future online safety developments. • Be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. • 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. • Provides training and advice for staff. • Liaise with school technical staff.

	• Liaises with local authority/MAT/relevant body. • Receive regular updated training to allow them to understand how digital technologies are used and are develop with regard to the areas defined in KCSIE-content, contact, conduct and commerce.
Computing Subject leaders	• leading role in establishing and reviewing the school's online safeguarding policy/documents. • Receive regular updated training to allow them to understand how digital technologies are used and are developing with regard to the areas defined in KCSIE – Content – Contact – Conduct – Commerce • work with senior leaders to develop a planned and co-ordinated online safety education programme e.g., ProjectEVOLVE. This will be provided through. – A discrete programme – PSHE and SRE programmes – A mapped cross-curricular programme – Assemblies and pastoral programmes – Through relevant national initiatives and opportunities e.g., safer internet day and anti-bullying week.
IT Network Manager	• They are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy. • That the school's technical infrastructure is secure and is not open to misuse or malicious attack • That the school meets the required online safety technical requirements as identified by the DfE meeting Digital and Technology Standards in Schools and Colleges and guidance from local authority/MAT or other relevant body. • 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 for investigation and action. • That monitoring software/systems are implemented and updated as agreed in school policies. • The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person • Meet weekly with the school health and safety officer to monitor the filtering.
Teachers and support staff	• They have an awareness of current online safety matters/trends and of current school Online safety policy and practices. • They understand that online safety is core part of safeguarding. • They have read, understood, and signed the staff Acceptable use Agreement (AUA) • They immediately report and log any suspected misuse or problem to the DSL for investigation/action in line with school safeguarding procedures.

	• Ensure that all digital communications with pupils/parents/carers is on a professional level and only carried out on 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, have a good understanding or 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 should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. • Where lessons take place using live streaming or video conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Remote Learning Resource. • Have 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 social media. **Exit strategy.** **At the end of a period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving ID's and passwords to allow devices to be reset, or meeting with line manager or IT Network Manager on the last day to log in and allow factory reset.**
All staff, volunteers, and contractors	• To read, understand, sign, and adhere to the school Acceptable Use Agreement document (AUA). The document is signed by new staff on induction. • To report any suspected misuse or problems to a DSL. • To maintain an awareness of current online safeguarding issues and guidance. • To model safe, responsible, and professional behaviours of their own use of technology. • There is an expectation that required professional standards will be applied to online safety as in any other aspect of school life using officially sanctioned mechanisms. **Exit strategy.** **At the end of a period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving ID's and passwords to allow devices to be reset, or meeting with line manager or IT Network Manager on the last day to log in and allow factory reset.**
Pupils	• Are responsibly for using the school 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 worried or vulnerable when using online technology.

	• To understand the importance of adopting good online safety practice when using behaviours and good online practice when using digital technologies out of school and realise that the school's online safeguarding policy covers their actions outside of school if related to their membership of the school.
Parent/Carers	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 learners' acceptable use agreement. – Publish information about appropriate use of social media relating to posts concerning the school. – Seeking their permissions concerning digital images, cloud services etc – Parents/carers evenings, newsletters, websites, social media and information about national/local online safety campaigns and literature. Parents and cares will be encouraged to support school in: – Reinforcing the online safety messages provided to learners in school.
External groups including parents' groups.	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the internet within school. • To support the school in promoting online safeguarding • To model safe, responsible, and positive behaviours in their own use of technology.

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 official sanctioned school mechanisms.

Policy Statements

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:

- Set expectations for the safe and responsible use of digital technologies for learning, administration, and communication for all members of the school community at Deepdale Community Primary School.
- Allocates responsibilities for the delivery of the policy.
- Is regularly reviewed in a collaborative manner, taking account on 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 a 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 such as in person meetings, email, and school network safeguarding folder.
- Is published on the school website.

Acceptable User Agreement (AUA)

The Online Safety Policy and acceptable use agreement define acceptable use at school. AUA's are recommended for all Staff, Pupils and Visitors/Guests and must be signed and understood by users before access to technology is allowed (see appendices 1, 2, and 3). Any breeches of Acceptable Use Agreements may result in further disciplinary action in accordance with Part 2: Personal and Professional Conduct, of the Teacher Standards. We consider AUA's as partnerships between parents/carers, pupils, and the school to ensure users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology must be kept in school and be made available to all staff. When using communication technologies, the school considers the following to be 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 must be professional in tone and content. Personal e-mail addresses, text messages 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 DSL-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.

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.
- 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 DSL 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 of serious harm (see appendix 5) 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
- Child 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 Head teacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority/MAT.
- Where there is no suspected illegal activity, devices may be checked using the following procedures.
  - One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
  - Conduct the procedure using the designation 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 describing the nature 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 any 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 disciplinary procedures
    - Involvement by the local authority/MAT
    - 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 for those reporting or affected by an online safety incident.
- Incidents should be logged on CPOMs using the online safeguarding incident tab.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues e.g., local authority, police, CEOP.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.
- Learning from the incident or pattern of incident will be provided to:
    - The online safety group for consideration of updates to policies or educational programmes
    - Staff through regular briefings
    - Learners through assemblies/lessons
    - Parents/carers through newsletters, school website
    - Governors through regular safeguarding updates
    - Local authority/external agencies as appropriate

Please see appendix 4 for online safety incident flowchart.

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Leaners need the help and support of the school to recognise and avoid online safety risks and develop their resilience. Including that we teach our children to follow a healthy balanced digital diet and endeavour to promote the Children's Commissioners Digital 5 a day campaign.

As highlighted in KCSIE para 20, 24-28. All school and college staff should be aware that abuse, neglect, and safeguarding issues are rarely standalone events that can be covered by one definition or label. In most cases, multiple issues will overlap one another.

- **Abuse**: a form of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm or by failing to act to prevent harm. Harm can include ill treatment that is physical as well as the impact of witnessing ill treatment of others. This can be particularly relevant, for example, in relation to the impact on children of all forms of domestic abuse, including where they see, hear or experience its effects. Children may be abused in a family or in an institution or community setting by those known to them or, more rarely, by others. Abuse can take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults or by another child or children.

- **Physical abuse**: a form of abuse which may involve hitting, shaking, throwing, poisoning, burning, or scalding, drowning, suffocating, or otherwise causing physical harm to a child. Physical harm may also be caused when a parent or carer fabricates the symptoms of, or deliberately induces, illnesses in a child.

- **Emotional Abuse**: the persistent emotional maltreatment of a child such as to cause severe and adverse effects on the child's emotional development. It may involve conveying to a child that they are worthless or unloved, inadequate, or valued only insofar as they meet the needs of another person. It may include not giving the child opportunities to express their views, deliberately silencing them or 'making fun' of what they say or how they communicate. It may feature age or developmentally inappropriate expectations being imposed on children. These may include interactions that are beyond a child's developmental capability as well as overprotection and limitation of exploration and learning or preventing the child from participating in normal social interaction. It may involve seeing or hearing the ill-treatment of another. It may involve serious bullying (including cyberbullying), causing children frequently to feel frightened or in danger, or the exploitation or corruption of children. Some level of emotional abuse is involved in all types of maltreatment of a child, although it may occur alone.

- **Sexual abuse**: involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing, and touching the outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. Sexual abuse can take place online, and technology can be used to facilitate offline abuse. Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children. The sexual abuse of children by other children is a specific safeguarding issue in education and all staff should be aware of it and of their school or college's policy and procedures for dealing with it.

- **Neglect**: the persistent failure to meet a child's basic physical and/or psychological needs, likely to result in the serious impairment of the child's health or development. Neglect may occur during pregnancy as a result of maternal substance abuse. Once a child is born, neglect may involve a parent or carer failing to provide adequate food, clothing, and shelter (inclusion exclusion from home or abandonment); protect a child from physical and emotional harm or danger; ensure adequate supervision (including the use of inadequate caregivers); or ensure access to appropriate medical care or treatment. It may include neglect of, or unresponsiveness to, a child's basic emotional needs.

As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups. As highlighted in The Prevent Duty-June 2015 we must provide an environment which protects and educates our children to have "due regard to the need to prevent people from being drawn into terrorism under the PREVENT duty by identifying children who may be vulnerable to radicalisation and know what to do when they are identified". We need to educate our children to build their resilience to radicalisation by promoting fundamental British Values and enabling them to challenge extremist views. It is important to emphasise that the Prevent duty is not

intended to stop pupils debating controversial issues but provide a safe open space in which pupils and staff can understand the risks associated with terrorism.

Prevent

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. As a school, we need to ensure that suitable filtering is in place.
More generally, as a school we have an important role to play in equipping children and young people to stay safe online, both in school and outside. As highlighted in KCSE Annex B p159 (Sept 2024)
Children may be susceptible to radicalisation into terrorism. Similar to protecting children from other forms of harms and abuse, protecting children from this risk should be a part of a schools' or colleges' safeguarding approach.

Extremism is the vocal or active opposition to our fundamental values, including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. This also includes calling for the death of members of the armed forces.

Radicalisation is the process of a person legitimising support for, or use of, terrorist violence.

Terrorism is an action that endangers or causes serious violence to a person/people; causes serious damage to property; or seriously interferes or disrupts an electronic system. The use or threat must be designed to influence the government or to intimidate the public and is made for the purposes of advancing a political, religious, or ideological cause.

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

- A planned online safety curriculum for all year groups matched against a nationally agreed framework and regularly taught in a variety of context.
- 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., PSHE, Literacy, Art.
- It incorporates relevant national initiatives and opportunities for example Safer Internet Day and Anti-Bullying Week.
- 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.
- The online safety education programme is relevant and up to date to ensure the quality of learning and outcomes.

The breath of issues classified within online safeguarding is considerable but can be categorised in four main areas of risk that our school needs to be aware of are:

Area of Risk	Example of Risk.
Content: Children need to be taught that not all content is appropriate or from a reliable source.	• Exposure to illegal content • Exposure to inappropriate or harmful material, including pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.

	• Lifestyle websites, for example pro-anorexia/self-harm/suicide sites. • Hate or radicalisation sites. • Content validation: how to check authenticity and accuracy of online content such as fake news.
Contact: Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	• Grooming/manipulation or coercion to radicalise. • Adults posing as children. • Online bullying in all forms • Identity theft (including 'frape' – hacking profiles e.g.,) and sharing passwords
Conduct: Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.	• Privacy issues, including the disclosure of personal information, digital footprint, and online reputation. • Online bullying • Health and well-being-amount of time spent online (internet or gaming). • Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent image). • Copyright (little care or consideration for intellectual property or ownership-such as music or film).
Commerce: Children need to be made aware of in appropriate advertising, phishing, or financial scams.	• Fake links in emails. • Links that can then pose a risk to your system or network. • Free giveaways to gain your data. • Online competitions. • Advertising during YouTube videos or as part of free games in apps.

Staff, volunteer, and governor training

All staff receive regular online safeguarding training and understand their responsibilities, as outlined in this policy. Training will be offered as follows (KCSIE p144, Teaching online safety in schools p17 Reviewing and Maintaining Online Safety Principles, Prevent Duty Guidance para 63, 64).

- Provides a planned programme of formal online safety and data protection training is made available for all staff. This will be regularly updated and reinforced.
- The training will be an integral part of the school's annual safeguarding and data protection training for all staff.
- New staff will receive online safety training as part of the induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreement. It includes explicit reference to classroom management, professional conduct, online reputation, and the need to model positive online behaviours.
- The computing subject lead and IT Network Manager will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safeguarding policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The computing subject lead will provide advice/guidance/training to individuals as required.

Governors should take part in online safeguarding training/awareness sessions, with particular importance for those who are members of the online safeguarding group, involved with safeguarding child protection, health, and safety.

Our school:

- Will provide training delivered by the Local Authority or other relevant organisation (e.g., SWGfL)
- Provide the opportunity to participate within school training/information sessions for staff and/or parents.

Families

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

The school will therefore seek to provide information and awareness to parents and cares 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
- The pupils-who are encouraged to pass on to parents the online safety messages they have learned in lessons and by pupils leading sessions at parents' evenings.
- Letters, newsletters, and the website
- Parents/carers sessions/workshops
- High profile event such as online safety day/week, anti-bullying week
- Reference to relevant websites/publications
- Sharing good practice with other schools in clusters and or the local authority/MAT.

Adults and Agencies

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

- Online safety messages targeted towards families and relatives.
- Providing family learning courses in the use of new digital technologies, digital literacy, and online safeguarding.
- The school website will provide online safeguarding information for the wider community.
- Sharing their online safety expertise/ good practice with other local schools.

Technology

Our school will ensure that our infrastructure /network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Our school subscribes to EXA Networks broadband; internet content filtering service is provided by EXA Networks SurfProtect. It is important to note that the filtering service offers a high level of protection, but occasionally unsuitable content may get past the filter service (further information can be found on the following webpage https://surfprotect.co.uk/education/ .

Sophos Intercept X Anti-Virus software is included in the school's subscription, and this has been installed on all computers and laptops in school and configured to receive regular updates.

Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Network Manager 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 Network Manager to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT Network Manager will have technical responsibility.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, IT Network Manager, and the safeguarding governor.

- Checks on the filtering and monitoring systems are carried out by the IT Network Manager with the involvement of a senior leader, DSL, and a governor particular when a safeguarding issue is identified.
- The school manages access to content across its systems for all users and on all devices using the school's 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 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 4)
- Filtering logs are regularly reviewed and alert the DSL to breaches of the filtering policy, which are then acted upon.
- The school has provided enhanced/differentiated user-level filtering.
- 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.

The school uses Securus as its monitoring system 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 DSL, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre guidance and protects users and the school systems through the appropriate blend of strategies informed by

- 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.

Technical security:

Our school has a managed technical service provided by an outside contractor (Schools' ICT Services) and Lancashire Education Services which manages the administration of SiMs, we as a school ensure that the managed service provider carries out all the online safeguarding measures that would otherwise be the responsibility of the school as outlined below.

- Responsibility for technical security resides with the 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 Network Manager and will be reviewed, at least annually by the Online Safety Group.
- Password policy and procedures are implemented.
- 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 systems will be protected by secure passwords. Passwords must not be shared with anyone.
- The administrator account passwords for the school 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 are regular reviews and audits of the safety and security of the school technical systems.
- Servers, wireless systems, and cabling must be securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, 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 copies off-site or in the cloud.
- The computing leads and the school IT Network Manager are responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- The IT Network Manager's online helpdesk is the appropriate system that is in place within school for users to report any actual/potential technical incident/security breach.
- The use of school devices outside of school is regulated by the school's acceptable user agreement.
- Personal use of any device on the school network is regulated by acceptable user statements that a user consents to when using the network.
- Staff members are **NOT** permitted to install software on school-owned devices without the consent of the SLT/IT Network Manager.
- We are **not** able to use pen drives to store data. Any data file that is saved will be encrypted or password protected for use outside of the school premises.
- Systems are in place to control and protect personal data. Data is also encrypted at rest and transit.
- We have an agreed policy in place for the provision of temporary access onto the school systems with a school owned laptop.

Mobile Technologies

School owned mobile technology devices include tablets, laptops. These devices have access to the school network and wireless system. The primary purpose of these devices in a school context is educational. The acceptable user agreements for staff, learners, parents, and carers outline the expectations of the use of mobile devices within school. The school allows the following devices and access to networks within school.

	SCHOOL DEVICE		PERSONAL DEVICE		
	School owned for individual use	School owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	YES	YES	NO	YES	YES
Full network access	YES	YES	NO	NO	NO
Internet only	NO	NO	NO	NO	YES If software installed onto device.

Use of own devices

However, there are several safety issues that need to be investigated prior to the use of any outside device by staff. Most importantly these devices should not introduce vulnerability into an existing secure environment. For this reason, at this point in time there is only very limited use of these type of devices in close consultation with the school IT Network Manager and computing leaders and they must follow the following criteria.

- No data, photographs or video will be stored on these devices and adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement
- All devices will be covered by the school's filtering systems while being used on the premises.
- No access to the school network or wireless network.
- No pupil owned devices will be permitted use on school premises.
- Regular audits and monitoring of usage will take place to ensure compliance.
- Any loss, damage, theft, will be the responsibility of the owner of the device.
- Children are **NOT** allowed mobile phones on school premises. These will be taken from the child by the class teacher and either returned to parent directly or placed in a secure place and returned to the parent at the end of the day.
- Staff must **NOT** use personal devices such as smart phones, personal iPads, or tablets to download e-mails from a school e-mail address that contains data unless password protected.
- Staff must **NOT** use own personal SD cards or personal mobile phones to take photographs of children within the school or on trips. Staff are permitted to use personal camera **ONLY** if a school SD card is used and removed once the event has finished.
- For use of mobile phones for staff, visitor and pupils please refer to the Mobile Phone policy.

Social Media

All schools have a duty of care to provide safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, online bully, discriminate on the grounds of sex, race, disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff, and the school through:

- Ensuring that personal information is not published.
- Education/training 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 assessments, including legal risks.
- Guidance for learners, parents/carers

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers, or school staff.
- They do **NOT** engage in online discussion or 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 or personal information.
- They act as a positive role model in their use of social media.

When official school social media account (X formerly known as Twitter, ClassDojo) is in use we adhere to the following.

- Approval of posts by the SLT.
- Clear process for the administration, moderation and monitoring of these accounts- involving at least two members of staff.
- Code of behaviour for users of the accounts
- Systems for reporting and dealing with the 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 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 outside of their directed hours, in private areas of the school where pupils are not present, discreet, and appropriate.

Monitoring of public social media:

- As part of active social media engagement, the school may proactively 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 procedure.
- When parent/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 procedures.

School use of social media for professional purposes will be checked regularly by a senior leader to ensure compliance with the social media, data protection, communications, digital image, and video policies.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers, pupils need to be aware of the risks associated with publishing digital images on to the internet. Such images may provide avenues for online bullying to take place (KCSIE para 22, 24, 26, 27). 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 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 should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet for example on social media sites.
- 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.
- Photographs and videos of pupils and staff are regarded as personal data in terms of The Data Protection Act (2018), and we have written permission for their use from the individual and/or their parents or carers. Each parent signs a photograph letter for each of their children at the beginning of each academic year. Any amendments can be made within the year by the parent or carer contacting the school office.
- Parents and carers that are invited to school events need to be made aware at the beginning of each event that the use of mobile phones and taking photographs during the performance is discouraged but there will be time at the end to take photographs at the end of their own child 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 pupils in the digital images. Where parents have breached these rules, parents will be asked to delete the images.
- Students or volunteers within school should check with the class teacher for which children parental consent has been granted for students/volunteers to take and use photographs. The photographs taken will only be used as evidence of work undertaken within the school and where possible students and volunteers should avoid taking photographs of children.
- Care should be taken when sharing digital/video images that learners are appropriately dressed.
- Pupils **MUST NOT** take, use, share, publish or distribute images of others without their permission.
- Photos published on the school website or ClassDojo will be selected carefully and comply with the Online safety policy.
- Digital images **MUST** be stored on the school network, class section of the network, My Pictures. If on a teacher's laptop it **MUST** be a school laptop and **MUST** be password protected. No digital images must be stored on **personal** devices for example mobile phones, cameras, laptops.
- Once children leave the school **MOST** photographs will be deleted the year after they have left. Some photos will be kept longer such as prospectus photos, special celebrations, class photos, whole school photos, special events (centenary) these will be kept as a historical record of these events.
- Staff and pupils are aware that full names and personal details will **NOT** be used on any digital media, particularly in association with photographs.
- Where photos of children are being shared with parents on ClassDojo staff must be aware of other children in the background of the photo and pixelate other children's faces within the photo, so they are not recognisable.
- All staff have been made aware of Social Networking Sites and been provided with Lancashire's advice on this. Staff **MUST NOT** use photographs taken on school premises on personal social networking sites.
- Staff **MUST** only use school equipment to take photographs of children and used for school purposes and photos should be deleted when no longer needed.
- Pupil's work can only be published with permission of the pupil and parents/carers.

Remote Learning

We will be ensuring constituency in the approach to remote learning for all pupils who are not in school using quality online and offline resources and teaching videos. Please see Deepdale remote learning plan for details of specific online learning platforms to be used and information above regarding the use of virtual learning platforms, video conferencing and use of mobile phones.

Online Publishing

The school communicates with parents/carers and the wider community and promotes school through a public facing website and X (formerly known as Twitter). The school website is managed by Schudio and hosted by EXA. 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

there is least risk to members of the school community, through such publications. Where learner work, images or videos are published, their identities are protected, and full names are not published.

Closed Circuit Television (CCTV)

We have CCTV in school as part of our site surveillance for staff and pupil safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission. The video from the CCTV is kept for a limited time and then it will be deleted.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation (GDPR). This data must be.

- Accurate
- Secure
- Fairly and lawfully processed.
- Processed for limited purposes.
- Processed in accordance with the data subject's rights.
- Adequate, relevant, and not excessive
- Kept no longer than necessary.
- Only transferred to others with adequate protection.

The school ensures that:
Data is kept secure, and all staff are informed as to what they can/cannot do regarding data in the following ways:

- All staff are aware of the Data Protection Policy.
- Implement the data protection principles outlined above, and we can demonstrate that we do through the use of policies, notices, and records.
- Has paid the appropriate fee to Information Commissioner's Office (ICO) and included details of the Data Protection Officer.
- Has a Data Protection Officer who has effective understanding of data protection law and is free from any conflict of interest.
- Has a "Record of Processing Activities" in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
- The Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed.
- Has an "information asset register" in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
- Information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed.
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school "retention schedule" supports this.
- Data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check the accuracy of the data we hold as suitable intervals.
- We provide staff, parents, volunteers with information about how the school looks after their data and what their rights are in a clear Privacy Notice.
- There are procedures in place to deal with the individual rights of the data subject.
- We carry 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.

- It has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors where personal data is protected.
- We understand how to share data lawfully and safely with other relevant data controllers.
- We have clear and understood policies and routines for the deletion and disposal of data.
- It reports any relevant breaches to the Information Commission within 72 hours of becoming aware of the breach in accordance with UK data protection law. We will also report relevant breaches to the individuals affected as required by law.
- We have a freedom of information policy which sets out how it will deal with the FOI requests.
- All staff receive data protection training at induction and appropriate refresher training thereafter.

When personal data is stored on a mobile device (school laptop) or removable media the:
- Data will be encrypted, and password protected.
- Device is 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 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 personal data to personal devices.
- Use personal data only on secure password protected computers and other devices ensuring that they are properly "logged-off" at the end of a session in which they are using personal data.
- Transfer data must use encryption, a secure e-mail account 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, learners, parent/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.

Deepdale Community Primary School would like to acknowledge the use of the SWGfL Online Safety Policy Template in the writing of this policy.

Appendix 1

ICT Acceptable Use Agreement (AUA) – Pupils Agreement-EYFS/KS1.

This is how we stay safe when we use computers:

- ✓ I will ask a teacher or suitable adult if I want to use the computers/tablets.
- ✓ I will only use activities that a teacher or suitable adult has told or allowed me to use.
- ✓ I will take care of the computers/tablets and other equipment.
- ✓ I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- ✓ I will tell a teacher or suitable adult if I see something that upsets me on screen.
- ✓ I know that if I break the rules, I might not be allowed to use a computer or tablet.

……

Parent/Carer Signature

We have discussed these rules and……. [Print Child's Name] agrees to follow them and support safe use of technology at Deepdale Community Primary School.

Parent/Carer Name (Print)……

Parent/Carer (Signature)…….

Class……Date…….

This form must be signed and returned to school before any access to the school ICT systems is allowed.

Appendix 2

ICT Acceptable Use Agreement (AUA) – Pupils Agreement-KS2.

When I use devices, I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- ✓ I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly.
- ✓ I will only visit internet sites that adults have told me are safe to visit.
- ✓ I will keep my username and password safe and secure and not share it with anyone else.
- ✓ I will be aware of "stranger danger" when I am online.
- ✓ I will not share personal information about myself or others when online.
- ✓ If I arrange to meet people off-line that I have communicated with online, I will do so in a public space and take a trusted adult with me.
- ✓ I will immediately tell and adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the device I use, so that the school and everyone there can be safe:

- ✓ I will handle all devices carefully and only use them if I have permission.
- ✓ I will not try to alter the settings on any device or try to install any software or programmes.
- ✓ I will tell an adult if a device is damaged or if anything else goes wrong.
- ✓ I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

- ✓ When online, I will act as I expect others to act towards me.
- ✓ I will not copy anyone else's work or files without permission.
- ✓ I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- ✓ I will not take or share images of anyone without their permission.

I know there are other rules I need to follow:

- ✓ When I am using the internet to find information, I should take care to check the information is accurate, as I understand that the work of others may not be truthful and may be deliberate attempt to mislead me.
- ✓ I should have the permission if I use the original work of others in my own work.
- ✓ Where work is copyright protected, I will not try to download copies of it (including videos and music).

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

- ✓ I know that I am expected to follow these rules in school and that I should behave in the same way when out of school.
- ✓ I understand that if I do not follow these rules, I may not use technology in school for a set period of time.

Parent/Carer Signature

We have discussed these rules and……. [Print Child's Name] agrees to follow them and support safe use of technology at Deepdale Community Primary School.

Parent/Carer Name (Print)……

Parent/Carer (Signature)…….

Class……Date…….

This form must be signed and returned to school before any access to the school ICT systems is allowed.

Appendix 3

ICT Acceptable Use Agreement (AUA) –All staff and volunteer 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 technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to the use of these technologies (e.g., laptops, e-mail, ClassDojo) out of school, and 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 devices and systems for this purpose.
- I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write it down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other's 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 ClassDojo or Website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school outside of my directed hours, in private areas of the school where pupils are not present.
- I will only communicate with learners and parents/cares using official school systems. Any such communications will be professional in tone and manner.
- I will not engage in any on-line 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 use personal email addresses 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 (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- I will not try to upload, download, or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other uses from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause damage to school equipment or equipment belonging to others.
- I will only transport, hold, disclose, or share personal information about myself or others, as outlined in the Data Policy. Where digital personal data is transferred outside the secure network, it must be encrypted. Paper based documents containing personal data must be kept securely and disposed of appropriately as soon as possible.
- I understand that data protection policy requires that any staff or learner 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 or 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 responsibly for my actions on 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 equipment off the premises.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action.

User Signature

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

Signature …… Date……

Full Name (PRINT)…….

Position/Role…….

Appendix 4

Deepdale Community Primary School.

Filtering Amendment Log.

Amendments to the filtering will be logged below and reviewed on a regular basis.

Date request made	Requested by who?	URL and reason	Date request was actioned.

Appendix 5 – Responding to online safeguarding Incident/Escalation Procedures.

Taken from SWGfL online safety policy template 2023.