The Meadows School

Online Safety Policy

Updated:	October 2023
Date to be reviewed:	October 2024
Ratified by Governors:	November 2023

Amendment Register

Amendment Number	Date	Detail	Amended By	Approved By
0	14/02/2023	Initial Issue	Stewart Harris/Theodora Papaspyrou	Headteacher
1	06/10/23		Theodora Papaspyrou (Acting HT and DSL)	

Table of Contents

1. Policy Aims

At the Meadows School we are committed to safeguarding and promoting the welfare of all pupils as the safety and protection of children is of paramount importance to everyone in this school. We work hard to create a culture of vigilance and at all times we will ensure what is best in the interests of all pupils.

We believe that all pupils have the right to be safe in our society. We recognise that we have a duty to ensure arrangements are in place for safeguarding and promoting the welfare of pupils by creating a safe online environment. We want all pupils to feel safe at all times.

We acknowledge that online safety:

- refers to the act of staying safe online and is also commonly known as internet safety, e-safety, and cyber safety. It encompasses all technological devices which have access to the Internet from PCs and laptops to smartphones and tablets. Being safe online means individuals are protecting themselves and others from online harms and risks which may jeopardize their personal information, lead to unsafe communications, or even effect their mental health and wellbeing.' (National Online Safety)

- is being aware of the nature of the possible threats that anyone could encounter whilst engaging in activity through the Internet, these could be security threats, protecting and managing your personal data, online reputation management, and harmful or illegal content.' (Southwest Grid for Learning)

We work hard to ensure that pupils are safeguarded from potentially harmful and inappropriate online material. We understand that there are many online safeguarding issues that can be categorised into four areas of risk:

Content:	Being exposed to illegal, inappropriate, or harmful material such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
Contact:	Being subjected to harmful online interaction with other users such as child-to-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
Conduct:	Personal online behaviour that increases the likelihood of, or causes, harm such as making, sending and receiving explicit images.
Commerce:	Risk such as online gambling, inappropriate advertising, phishing and of financial scams

We believe online safety:

- is an integral part of safeguarding and requires a whole school, cross-curricular approach.
- must follow the school's safeguarding and child protection procedures.
- will educate pupils about the benefits and risks of using technology.
- will provide safeguards and awareness to enable pupils to control their online experience.

We aim:

- To safeguard and promote the welfare of all pupils as the safety and protection of children is of paramount importance to everyone in this school.
- To ensure arrangements are in place for safeguarding and promoting the welfare of pupils by creating a safe online environment.
- To create a culture of vigilance and at all times ensure what is in the best interests of all pupils.
- To ensure compliance with all relevant legislation connected to this policy.
- To share good practice within the school, with other schools and with the local authority in order to improve this policy.

This policy applies to all members of the school community (including staff, governor's, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of school.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy operates in conjunction with the following school policies:

- The Meadows School Acceptable Use Agreement
- The Meadows School Child Protection and Safeguarding Policy
- The Meadows School RSE and Health Education Policy
- Staff Code of Conduct
- The Meadows School Behavioural Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- The Meadows School Remote Learning Policy
- Prevent Policy
- Complaints procedure

3. Roles and Responsibilities

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that are connected with this policy.

4. Role of The Governing Body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Governing Body will nominate a governor to oversee online safety. The nominated Governor is **Mr Phillip Butcher.**

All governors will:

- Ensure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (see appendices).
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special

educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

All governors will ensure that they have read and understand this policy and will agree and adhere to the terms on acceptable use of the school's IT systems and the internet. (See appendices - **Acceptable Use of Technology)**

5. Role of the Head teacher

The headteacher will:

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

6. Role of the Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in the safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

7. Role of the Data Protection Officer

The data protection officer will:

- have expert knowledge of data protection law and practices.
- inform the school and school personnel about their obligations to comply with the Data Protection Act 2018 laws.
- ensure data management is strengthened and unified.
- monitor compliance with the Data Protection Act 2018.
- manage internal data protection activities.
- ensure risk and impact assessments are conducted in accordance with ICO guidance.
- report data breaches.
- ensure individuals have greater control over their personal data.
- ensure that prior to the processing of an individual's data that:

✓ the process is in line with ICO guidance.
✓ the process is transparent.
✓ he individual will be notified.
✓ the notification is written in a form that is understandable to children.
✓ when sharing an individual's data to a third party outside of school that details for the sharing are clearly defined within the notifications.

- share an individual's data where it is a legal requirement to provide such information.
- process all written subject access requests from individuals within 40 days of receiving them.
- have in place a formal contract or service level agreement with a chosen data processor who is GDPR compliant.
- ensure the secure disposal of redundant data and IT hardware holding data in compliance with ICO guidance.
- train school personnel.
- conduct audits.
- be the first point of contact for supervisory authorities and for individuals whose data is processed.
- keep up to date documentation of all data protection activities.
- work closely with the headteacher and nominated governor.
- periodically report to the headteacher and to the governing body.
- annually report to the governing body on the success and development of this policy.
- promote and model positive online safety behaviour.

8. Role of The IT Manager

The IT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep Students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a monthly] basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Helping to ensure that any online safety incidents are logged and dealt with appropriately.
- ensure all users access the Internet in accordance with the school's acceptable Internet use agreement and will inform the ICT coordinator if at any time they find they have accessed inappropriate Internet sites.
- ensure the technical infrastructure is secure and not open to misuse or malicious attack.
- ensure the online school meets all online safety technical requirements.
- keep up to date with online technical information.
- promote and model positive online safety behaviour.

This list is not intended to be exhaustive.

9. Role of Members of Staff

Members of staff will:

- comply with all aspects of this policy.
- be fully aware of all online safeguarding policies and procedures.
- undertake online safeguarding training on induction and when necessary.
- report all suspected safeguarding concerns and disclosures to the Designated Safeguarding Lead
- ensure all communications with pupils and parents will be on a professional level.
- read, understand, and sign the online safeguarding policy.
- reinforce online safety messages when teaching online.
- be aware that RSHE, computing and citizenship have the clearest online safety links.
- identify opportunities to thread online safety through the curriculum and other school activities.
- monitor what pupils are doing and consider potential online dangers.
- supervise and guide pupils when engaged in online learning activities.
- teach all pupils as appropriate to:

- ✓ be critically aware of the materials/content they access online and will show how to validate the accuracy of information.
- ✓ report abuse or any form of online bullying.
- ✓ be vigilant against online radicalisation.
- ✓ acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- ✓ demonstrate appropriate online behaviour.
- ✓ consider potential risks and the age-appropriateness of websites.
- ✓ create a safe online environment for their pupils.
- remind pupils to follow the acceptable use policy.
- promote and model positive online safety behaviour.
- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that Students may be unsafe online.

- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

10. Role of Parents

Parents /Carers will:

- Be aware of and comply with this policy.
- Work in partnership with the school
- Be made aware that they play an essential role in the online education of their children. There is an Online Safety section on the school website dedicated to providing parents information on Online Safety.
- Be expected to sign the acceptable use agreement and will be encouraged to adopt safe and responsible use of the internet.
- Promote and model positive online safety behaviour.
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with Designated Safeguarding Lead Team.

11. Role of Visitors including volunteers and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

12. Role of Students

The Meadows School is a school for students with a range of special educational needs and is aware that some students are more vulnerable online due to a range of factors. This may include but is not limited to children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. We recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation. We acknowledge that all Students are vulnerable to exploitation and the impacts of using technology and therefore we differentiate accordingly to meet the individual needs of all learners. This means that the life experiences and the communication need of our students and their families must be considered carefully when implementing the policy.

Students

- Are responsible for using the school IT systems in accordance with the Student / Student Acceptable Use Agreement, which they will be expected to agree to before being given access to school systems- where appropriate for age and ability.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so-where appropriate for age and ability.
- Will be expected to follow school rules relating to this policy e.g., safe use of cameras, cyber-bullying etc.
- Should understand that the school's online safety Policy covers their actions out of school, if related to their membership of the school- where appropriate for age and ability.

13. Safeguarding

We:

- are committed to safeguarding and promoting the welfare of all children as the safety and protection of children is of paramount importance to everyone in this school.
- work hard to create a culture of vigilance and at all times we will ensure what is best in the interests of all children.
- believe that all children have the right to be safe in our society.
- recognise that we have a duty to ensure arrangements are in place for safeguarding and promoting the welfare of children by creating a positive school atmosphere through our teaching and learning, pastoral support, and care for both pupils and school personnel, training for school personnel and through working with parents.
- teach all our children about safeguarding.
- work hard to ensure that everyone keeps careful watch throughout the school and in everything we do for possible dangers or difficulties.
- want all children to feel safe at all times.
- want to hear their views of how we can improve all aspects of safeguarding and from the evidence gained we put into place all necessary improvements.
- ensure that all school personnel:

✓ who work directly with children must read Part One of 'Keeping Children Safe in Education' (KCSiE) guidance.
✓ who do not work directly with children can either read Part One or Annex A.
✓ must understand their roles and responsibilities.
✓ must:

- understand that safeguarding and promoting the welfare of children is everyone's responsibility.
- attend appropriate safeguarding and child protection training at induction.
- be made aware of the following policies:

✓ Safeguarding and Child Protection
✓ Behaviour
✓ Staff Code of Conduct
✓ Role of Designated Safeguarding Lead (DSL)as included in the Safeguarding and Child Protection Policy.
✓ Attendance Policy for Students

- attend regular updated safeguarding training.
- be aware of all safeguarding systems within the school.
- be in a position to identify concerns early, provide help for children, promote children's welfare, and prevent concerns from escalating.
- have responsibility to provide a safe environment in which children can learn.
- be prepared to identify children who may benefit from early help.
- follow the processes as set out in KCSiE (paragraphs 51-67) if they have any concerns about a child's welfare.
- be aware of the process for making referrals to the local authority.
- support social workers and other agencies following any referral.
- report to the designated safeguarding lead any concerns they have regarding a child.
- know what to do if a child tells them they are being abused, exploited, or neglected.

- be able to reassure victims that they are being taken seriously and that they will be supported and kept safe.
- be familiar with 'Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children (DfE)'.

14. Online Filtering and Monitoring

We take very seriously our responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, and implementing filtering and monitoring systems and processes is a key part of this. We adhere to the government standards published in: Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) Filtering and Monitoring systems enable us to limit as much as possible, children's exposure to the online risks from the school's IT system.

At this school, we use the following system/s: **SENSO.**

Online Safety and Filtering and Monitoring is the responsibility of the DSL.

Theodora Papaspyrou (Acting Head Teacher & DSL) has lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place.

The DSL is supported in this by the governing body and together, they review the effectiveness of the systems, at least on an annual basis. We use a range of tools to help us review, including the Prevent Duty risk assessment.

It is vital that Filtering and Monitoring helps us to keep children safe but does not lead to 'over blocking' – creating unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding. Examples could be children being unable to access factual information relating to a project or being blocked from accessing helpful resources and websites to seek support. Staff working with children are in key positions to notice if there are any concerns and to escalate these immediately to the DSL, recognising them as a potential safeguarding concern. Examples of this include (but are not limited to):

• Spotting or overhearing that students have managed to override a system and access inappropriate content online.

• Spotting or overhearing students being able to use slang terms that are not recognised by the filtering and monitoring system and using these to search for and access inappropriate content.

• Spotting that inappropriate settings have been placed on video-sharing sites such as YouTube enabling for harmful or inappropriate videos to be accidentally shared with students.

Our filtering and monitoring system sends us daily alerts of when a child may have attempted to access harmful or inappropriate content. These are monitored and responded to on a daily basis by: **Theodora Papaspyrou** (Acting Head Teacher and DSL)

In their absence, the member/s of staff who will take on this responsibility are: **Stewart Harris** (Assistant Head Teacher).

Upon receiving a filtering and monitoring alert or notification, the DSL or a deputy will consider whether there is any risk to the child or whether further support may be necessary, taking into

account any contextual or historical concerns on the child's safeguarding file, or any current risk assessments. Action may be taken, as with any safeguarding concern, including (but not limited to):

- Liaison with other professionals working with the child such as Police, Children's Social Care, CAMHS/CYPMHS
- Liaison with parents/carers
- Actioning another member of staff such as a teacher or pastoral support team to speak further with the child and explore support options.

15. Educating pupils about online safety

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Personal, social, health and economic (PHSE) education
- Relationships, Sex and Health Education (RSHE)
- Online safety teaching is always appropriate to pupils' ages and developmental stages.
- Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform, or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:
    - How to evaluate what they see online
    - How to protect themselves online, including an awareness surrounding how data is stored, shared, and used.
    - How to recognise techniques used for persuasion and exploitation
    - What healthy and respectful relationships look like, especially in an online format
    - Body image and self-esteem, including reliability of the media and role models.
    - Consent, e.g., with relation to the sharing of indecent imagery, online coercion to perform sexual acts and sharing data.
    - Acceptable and unacceptable online behaviour
    - How to identify online risks
    - How, when, and where to seek additional support.
    - Health and well-being, e.g., reducing screen time for a healthy lifestyle and how too much can jeopardise physical and mental health.
    - How to identify when something is deliberately deceitful or harmful
    - How to recognise when something they are being asked to do puts them at risk or is age-inappropriate
    - The online risks pupils may face online are always considered when developing the curriculum, and medium-term plans are in place to support the delivery of this content.

The My Thinking Curriculum Lead and My Lifestyle lead are involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites, apps, and games they and their peers frequent and the kinds of behaviours in which they engage online.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g., designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the curriculum lead, class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

16. Remote Learning

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents

prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed and can establish secure connections.

During a period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g., sites they have been asked to use and staff they will interact with
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g., antivirus software, on devices not owned by the school.

17. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

The school will let parents know:

- ✓ What systems the school uses to filter and monitor online use
- ✓ What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with Designated Safeguarding Team.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

18. Cyber-bullying

18.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

19. Preventing and addressing cyber-bullying.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school safeguarding policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

20. Examining electronic devices.

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- ✓ Poses a risk to staff or pupils, and/or
- ✓ Is identified in the school rules as a banned item for which a search can be carried out, and/or
- ✓ Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- ✓ Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Head Teacher or DSL (or from a Senior Leader in their absence).
- ✓ Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- ✓ Seek the pupil's cooperation.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- ✓ Cause harm, and/or
- ✓ Undermine the safe environment of the school or disrupt teaching, and/or
- ✓ Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher /or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- ✓ They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- ✓ The pupil and/or the parent refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (**also known as a nude or semi-nude image**), they will:

- ✓ **Not view the image**

- ✓ Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- ✓ The DfE's latest guidance on searching, screening and confiscation
- ✓ UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

21. Acceptable use of the internet in school

All pupils, parents, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors, and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

22. Pupils using mobile devices in school.

· We recognise that mobile phones are part of everyday life for many children and that they can play an important role in helping students to feel safe and secure.

However, we also recognise that they can prove a distraction in school and can provide a means of bullying or intimidating others.

· Students are not permitted to have mobile phones at school or on trips

· Any mobile phone that has been brought into school will be confiscated immediately and handed back at the end of the school day.

· If in the rare event of a parent wishing for his/her child to bring a mobile phone to school to contact the parent after school:

- the parent must discuss the issue first with the head teacher.

- the phone must be handed in, switched off, to the office first thing in the morning and collected from the office by the child or class teacher at home time (the phone is left at the owner's own risk).

- Mobile phones brought to school without permission will be confiscated and returned at the end of the day

· If any member of staff has any suspicion that a mobile phone has been brought into school by a student and has unsuitable material stored on the device, the student will be required to hand it over to the staff member immediately and the parents will be asked to collect the phone from a member of SLT.

Please also refer to the Meadows School Mobile Policy.

23. Staff using work devices outside school.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- ✓ Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g., asterisk or currency symbol)
- ✓ Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- ✓ Making sure the device locks if left inactive for a period of time.
- ✓ Not sharing the device among family or friends
- ✓ Installing anti-virus and anti-spyware software
- ✓ Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use agreement.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from a member of the **Senior Leadership team.**

24. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, the action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct/disciplinary procedures. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

25. Training

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will cover the potential risks posed to Students (Content, Contact Conduct and Commerce) as well as our professional practice expectations.
- Make staff aware that school systems are monitored, and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.

- Highlight useful educational resources and tools which staff should use, according to the age and ability of the students.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting Students, colleagues, or other members of the school community.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and DDSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

26. Monitoring arrangements

The practical application of this policy will be reviewed annually or when the need arises by the Designated Safeguarding Lead, Online Safety Team and the nominated governor.

A statement of the policy's effectiveness and the necessary recommendations for improvement will be presented to the governing body for further discussion and endorsement.

Appendix A: Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation. • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services. • Install any unauthorised software or connect unauthorised hardware or devices to the school's network. • Share my password with others or log in to the school's network using someone else's details. • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community. • Access, modify or share data I'm not authorised to access, modify or share. • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix B: **Acceptable Use Agreement for Parents & Students.**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil): Print pupil Name:	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer): Print Name:	**Date:**