Our school is part of the Embark Federation.
The shared vision for our trust is to “create schools that ‘stand out’ at the heart of their communities.” Our trust has four core beliefs; Family, Integrity, Teamwork and Success that are integral to everything we do. The purpose is to enable everyone to be able to ‘Love Learning, Love Life.’
Our policies are underpinned by our vision, beliefs and purpose

Online Safety Policy and Procedures

Date of Issue	September 2025
Date of Review	September 2026
Version	V6
Approval Level	People and Remuneration Committee
Changes Made	Section 3: Volunteers updated and appendix added with the full induction checklist Section 4: Updated policy statement Section 12: Updated to reflect the implementation of My New Term Section 13: Updated to reflect the implementation of My New Term Section 15: References updated in line with EYFS Statutory Framework and inclusion of online checks.

This policy will be made available on the trust and school website.

Version	Reviewed /Modified by	Change History
5	Embark Safeguarding Lead – HJ	**Legal Framework** • Legislation, statutory and non-statutory guidance documents have been updated reflecting the latest versions. Web links have been updated. NB: there are no new legal frameworks or guidance documents. **Roles and Responsibilities** Added (in line with KCSIE 2024); ▪ All DSLs should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on: ➢ Filtering and monitoring reports ➢ Safeguarding concerns ➢ Checks to filtering and monitoring systems **Sexting** • Added link to DDSCP Online Safety and Internet Abuse procedures • Added information and link re NCMECs Take it down tool **Communications** • Amended table regarding pupil mobile phone use in social time – added school discretion column **Appendix 2: Annual online safety school audit and risk assessment tools** • Added links to two recommended free audit tools provided by LGFL and SWGFL
6	IT LEAD - LJ	• Referenced to DfE's "Generative AI: Product Safety Expectations" (Jan 2025) and the latest DfE AI policy paper and covered off what the trust will do to vet things. • Specified that filtering and monitoring systems must be reviewed to ensure they cover AI tools, including generative AI and chatbots • Require regular staff training on safe use of AI, risks (e.g., bias, misinformation, data privacy), and reporting concerns • Include guidance on teaching students about the risks of AI-generated content (misinformation, deepfakes, privacy, profiling), and critical thinking skills to identify fake news/conspiracy theories • Clarify that personal/sensitive data must not be entered into AI tools, and staff/students should be trained on this risk • State that filtering and monitoring systems must be reviewed at least annually, using the DfE's "Plan Technology for Your School" tool • Add requirement for a policy on responding to incidents identified through monitoring, including those involving AI

		• Explicitly list misinformation, disinformation, and conspiracy theories as online harms, as per KCSIE 2025 • Reference DfE Cyber Security Standards for Schools and Colleges, and require regular audits of digital resilience • Provide information to parents about AI risks, safe use, and how to support children in navigating AI-generated content • Ensure governors/Trustees receive regular updates on AI, filtering/monitoring, and online safety audit outcomes • Commit to reviewing and updating the policy annually, or sooner if significant changes in technology or statutory guidance occur. • Changes from Network Manager to IT Lead to make it clearer • Removed Sarah Armitage and changed all to David King

Contents
1. Introduction
2. Legal Framework
3. Roles and Responsibilities including prevent duties
4. Technical – Infrastructure, Equipment, Filtering and Monitoring
5. Use of Digital and Video Images including youth produce sexual imagery
6. Generative Artificial Intelligence (AI)
7. Sexting
8. Data Protection
9. Communications
10. Social Media – Protecting Professional Identity
11. Other incidents
12. School Actions and Sanctions
13. School Technical Security (including filtering and passwords)
14. Password Security
15. Filtering
16. See also other relevant policies

Appendix 1	**Pupil Acceptable Use Agreement template**
Appendix 2	**Annual Online Safety school audit and risk assessment Tools**
Appendix 3	**Responding to an Online Safety Concern Flow Chart**

1. Introduction

Our School understands that using online services and a range of devices both in school and for remote learning is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning.

Using online services and a range of devices safely can bring huge positive benefits in equipping children to navigate a rapidly advancing world. There needs to be a number of controls in place to ensure the safety of pupils and staff.

There are generally four areas of risk:

- Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.

- Contact: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

- Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

- Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff. This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

2. Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DFE (2024) 'Keeping children safe in education 2024'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Science, Innovation and Technology (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and

empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The Searching, Screening and Confiscation Advice for Schools 2022 increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The 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.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil/pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Un-authorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- The potential for excessive use may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

3. Roles and Responsibilities:

The following section outlines the online safety roles and responsibilities of staff, individuals and groups within the school.

We expect all staff to take responsibility for reporting searching for inappropriate content, any indicators devices in school may not have filtering or monitoring, and or searching has resulted in a surge on topics which may indicate risk/risky behaviours.

Trustees:

Trustees are responsible for ensuring that the trust have a robust online safety policy for the family of Embark schools and that policy is current and line with national policies and procedures. Schools need to ensure that governors know about this policy and have approved it.

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors, Headteacher and DSL receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor, this will include ensuring compliances to the DfE (2023) 'Meeting digital and technology standards in schools and colleges'

The role of the Online Safety Governor will also include:

- regular meetings with the Network Manager
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors / Board / committee / meeting

IT Lead / Technical staff:
The Network Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering process is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- That they keep up to date with online safety technical information in order to effectively carry out their role and to inform and update others as relevant
- That the use of the network, internet, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher, IT Coordinator and Online safety Governor for investigation/action/sanction
- That monitoring software/systems are implemented and updated as agreed in school policies
- The management of technical security will be the responsibility of the IT Lead

Head teacher and Senior Leaders, including Designated Safeguarding Lead (DSL):

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Designated Safeguarding Lead
- The Headteacher and (at least) another member of the Senior Leadership Team (SLT) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents)
- The Headteacher and SLT are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. This will include an awareness of cyber threats and cybercrime.
- The Headteacher and SLT 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. This

is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Headteacher and Online safety Governor will receive regular audit and monitoring reports, and will use this to identify risks, trends and activities
- The headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

Teaching and Support Staff are responsible for ensuring that:

- They have up-to-date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the EMBARK Trust Acceptable use of the Internet and Electronic Communication
- They report any suspected misuse or problem to the Headteacher and Network Manager for investigation/action/sanction
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- They monitor the use of digital technologies, mobile devices, cameras etc. in school and other activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils 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
- Identify students who are involved in cybercrime or those who are technically gifted and talented and are at risk of becoming involved in cybercrime
- The curriculum includes and recognises misinformation, disinformation and conspiracy theories as significant online harm.

Designated Safeguarding Lead

- All DSLs should have an understanding of the filtering and monitoring processes in place at the school.
- All DSLs should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:
  - Filtering and monitoring reports
  - Safeguarding concerns
  - Checks to filtering and monitoring systems
- All DSLs should undertake training in online safety at least every two years, one that includes cyber safety and security, be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

  - Searching by a pupil/pupils for materials, sites, social media platforms that may be considered harmful/misleading
  - Sharing of personal data
  - Access to illegal/inappropriate materials
  - Inappropriate online contact with adults/strangers
  - Potential or actual incidents of grooming
  - Cyber-bullying

Parents / Carers

Many parents and carers may have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will take every opportunity to help parents understand these issues

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

- Curriculum activities
- Letters, newsletters, website, physical resources
- Parents / Carers evenings / sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

Parents will be informed of the school's online safety policy through the Acceptable Use Agreement and through online safety awareness sessions/newsletter etc.

Information about keeping children safe online will be published on the school's website along with organisations where online abuse can be reported. All school websites will have the CEOP report abuse link.

The Wider Community

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

- Providing family learning in the use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- Partnership work with local schools.
- The school website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, youth/sports / voluntary groups to enhance their online safety provision.

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school
- Are expected to sign an age-appropriate Acceptable Use Agreement like the example in (Appendix 1)

Prevent duties

There are specific roles and responsibilities in the Prevent Duty Guidance: England and Wales, 2023 and which covers the possibility of online radicalisation and accessing terrorism social media platforms.

- All staff including trustees and governors will receive training that incorporates online safety and the Prevent Duty
- All reasonable precautions will be taken to ensure that pupils and all staff are safe from terrorist and extremist material when accessing the internet on the school site.
- If there are concerns that a pupil, parent/carer, a member of the local community may be at risk of radicalisation online, the Headteacher/ SLT/ DSL will be informed immediately, and action will be taken in line with our child protection policy and Derbyshire prevent pathway which may include a referral into Channel if that person is a child or young person.
- If there are concerns that member of staff or a staff member working on behalf of a school may be at risk of radicalisation online, the head teacher will be informed immediately, and action will be taken in line with the local child protection procedures and if relevant the Embarks Trust Managing Allegations and Concerns policy

Pupils - Education

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

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

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and are regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils are taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

- Staff act as good role models in their use of digital technologies the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that pupils 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 pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Pupils will also be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.
Staff users will be made aware of the filtering systems through:
- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Education and Training – Governors

Governors should take part in online safety training or awareness sessions, with particular importance for those who are members of any group involved in technology, online safety, health and safety or child protection. This may be offered in a number of ways:
- Attendance at training provided by the Embark Trust and this may mean online training
- Participation in school training or information sessions for staff or parents, this may include attendance at assemblies / lessons.

Education & Training – Staff / Volunteers

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:
- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly
- All new staff receive Online Safety and NCSC Cyber Security training (via Flick training modules) as part of their induction programme, ensuring that they fully understand the school's online safety policy and Acceptable Use Agreements.
- The DSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The DSL will provide advice/guidance/training to individuals as required

4. Technical – Infrastructure, Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- The "master/administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- The school has provided enhanced/differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc 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 virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- The trust will use the DfE "Plan Technology for Your School" tool to annually review filtering and monitoring systems, ensuring coverage of emerging technologies including AI. All incidents identified through monitoring will be managed according to the school's safeguarding procedures.

5. Use of 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 and carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents and carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents or carers comment on any activities involving other pupils in the digital or video images.
  Schools will inform parents and carers if they need to restrict photographs or videos from being taken at school events. It may not always be possible to explain why the decision has been made if there are confidential concerns, but it will not have been taken without good reason. In these circumstances, schools will endeavour to share pictures with parents and carers after the event
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes. Photos should be uploaded to the secure staff shared drive and images erased from any portable devices
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or social media channels
- Pupils' work can only be published with the permission of the pupil and parents or carers.

6. Generative Artificial Intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age. The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupils' ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI. The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

The school will follow the Department for Education's (DfE) Generative AI: Product Safety Expectations and ensure all AI tools used by staff and students are subject to appropriate filtering and monitoring. Schools can check AI services via the IT Support Team for approval and setup. Appropriate DPI assessments need to take place and be logged centrally. Staff and students must not enter personal or sensitive data into AI systems. Regular training will be provided on the risks of AI, including misinformation, bias, privacy, and safeguarding. The school will educate pupils on identifying AI-generated misinformation and conspiracy theories.

Link to the DfE AI: Product Safety Expectations

All staff will receive regular training on online safety, including the safe use of AI tools, cyber security, and the identification and reporting of online harms. Training will be updated annually and aligned with the latest statutory guidance via the trusts training platform.

The school will provide parents and carers with information about the risks associated with AI, including misinformation and data privacy. Resources and guidance will be shared through newsletters, workshops, and the school website to support safe use of AI at home.

7. Sexting (youth produced sexual imagery)

'Sexting' (youth-produced sexual imagery) is one of a number of 'risk-taking' behaviours associated with the use of digital devices, social media or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with 'online' activity can never be completely eliminated. However, the school takes a pro-active approach to help pupils to understand, assess, manage and avoid the risks associated with 'online activity'.

The school recognises its duty of care to pupils who find themselves involved in such activity as well as its responsibility to report such behaviours where legal or safeguarding boundaries are crossed.

Definitions

There are a number of definitions of 'sexting' but for the purposes of this policy sexting is simply defined as:

- Images or videos generated
  - by children under the age of 18
  - of children under the age of 18 that are of a sexual nature or are indecent
- These images are shared between young people and/or adults via a mobile phone, handheld device, computer, 'tablet', iPad or website with people they may not even know

It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence. Specifically, crimes involving indecent photographs (including pseudo images) of a person less than 18 years of age fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation, it is a crime to:

- take an indecent photograph or allow an indecent photograph to be taken;
- make an indecent photograph (this includes downloading or opening an image that has been sent via email);
- distribute or show such an image;
- possess with the intention of distributing images;
- advertise; and possess such images

“sexting” is classed as illegal as it constitutes sharing and/or possessing an indecent image of a child. However, it is rare that the police prosecute child on child incidents and will ways consider the circumstances e.g. power, control, coercion, ages, CRE/CSE.

Steps to take in the case of an incident

The school will follow the guidelines and steps taken as described in the following national guidance’s:

Sharing nudes and semi-nudes: advice for education settings working with children and young people (updated March 2024) - GOV.UK (www.gov.uk)

And the local safeguarding procedures as set out by the Derby and Derbyshire Safeguarding Children’s Partnership (section 1.7.17- Online safety and internet abuse) Online Safety and Internet Abuse (proceduresonline.com)

Cybercrime incidents

Cybercrime incidents and offences will be responded to in line with our existing behaviour policies. We will respond to concerns that our students are involved, or at risk of becoming involved, in cybercrime, even if it takes place off-site. Concerns that a child is being exploited as a result of their technical skills, we will follow the Children at Risk of Exploitation (CRE) procedure

Online bullying, online hate, extremism and radicalisation

Cyberbullying is a form of bullying and will not be tolerated. Full details are set out in our anti-bullying policy.

Online hate content, directed towards another pupil or posted will not be tolerated and will be responded to in line with existing policies, including anti-bullying and behaviour . The Police will be contacted if a criminal offence is suspected.

All reasonable precautions will be taken and in line with filtering and monitoring to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.

Disclosure by a pupil

“Sexting” disclosures should follow the normal safeguarding practices and protocols (see the schools Child Protection and Safeguarding Policy).

A pupil is likely to be very distressed, especially if the image has been circulated widely and if they don't know who has shared it, seen it or where it has ended up. They will need emotional support during the disclosure and after the event. They may even need immediate protection or a referral to police or social services; parents should be informed as soon as possible (police advice permitting).

The following questions will help staff decide upon the best course of action:

- Is the pupil disclosing about themselves receiving an image, sending an image or sharing an image?
- What sort of image is it?
- Is it potentially illegal or is it inappropriate?
- Are the school child protection and safeguarding policies and practices being followed?

For these reasons a member of the SLT should be involved, as soon as possible

- How widely has the image been shared and is the device in their possession?
- Is it a school device or a personal device?
- Does the pupil need immediate support and/or protection?
- Are there other pupils and/or young people involved?
- Do they know where the image has ended up?

Staff must always:

- Inform and involve the SLT who will ensure that the DSL (or Deputy DSL) is able to take any necessary strategic decisions.
- Record the incident. The SLT employs a systematic approach to the recording of all safeguarding issues.
- Act in accordance with school safeguarding search and confiscation policies and procedures

If there is an indecent image of a child on a website or a social networking site then the SLT will report the image to the site hosting it.

Under normal circumstances the team would follow the reporting procedures on the respective website; however, in the case of a "sexting" incident involving a pupil where it may be felt that they may be at risk of abuse then the team will report the incident directly to CEOP www.ceop.police.uk/ceop-report, so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child. NCMEC's Take It Down tool can also be used to help individuals anonymously remove nudes or semi-nudes that have yet to be shared online but they think might be (for example, in an incident where a young person has been threatened to have their image shared but threat has not yet been carried out): https://takeitdown.ncmec.org.

Who should deal with the incident?

Often, the first port of call for a pupil is a class teacher. Regardless of whom the initial disclosure is made to she/he must act in accordance with the school Safeguarding Policy,

ensuring that a member of the SLT (DSL) and a Senior member of staff are involved in dealing with the incident.

The DSL (or in their absence the Deputy DSL) should always record the incident. The Headteacher should also always be informed- usually by the DSL.

Deciding on a response

There may be many reasons why a pupil has engaged in "sexting" – it may be a sexual exploration scenario or it may be due to coercion.

It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident, however, as a school it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere.

If indecent images of a pupil are found:

- Act in accordance with the Embark Trust Safeguarding and Child protection Policy
- Store the device securely
- The SLT will assist the Deputy Head Care and Guidance to carry out a risk assessment in relation to the young person
- The SLT will make a referral (where necessary)

The SLT (DSL) will contact the police (if appropriate). Referrals may be made to Social Care. Where a crime may thought to have taken place the police are the first port of call.

Pupils who have engaged in 'experimental sexting' which is contained between two persons will be referred to other external agencies for support and guidance. Those who are felt to be victims of 'sexting' will also be referred to Social Care at a point where the police feel that this will not impede an investigation.

The DSL or Deputy DSL will inform parents and/or carers about the incident and how it is being managed and offer support to the pupil.

The pupil/s involved in 'sexting' may be left feeling sensitive and vulnerable for some time. They will require monitoring by and support from a key worker or support staff at the school.

Where cases of 'sexting' become widespread or there is thought to be the possibility of contagion then the school will reinforce the need for safer 'online' behaviour using a variety of resources. Other staff may need to be informed of incidents and should be prepared to act if the issue is continued or referred to by other pupils.

The school, its pupils and parents should be on high alert, challenging behaviour and ensuring that the victim is well cared for and protected. The pupil's parents should usually be told what has happened so that they can keep a watchful eye over the young person especially when they are online at home.

Creating a supportive environment for pupils in relation to the incident is very important.

Preventative educational programmes on sexting can be found on CEOP's advice-giving website; www.thinkunknow.co.uk and the South West Grid for learning have developed advice for young people at www.swgfl.org.uk/sextinghelp

There is also a lot of support and guidance for staff, pupils and parent/carers at NSPCC; https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/

8. Data Protection

- Personal data will be recorded, processed, transferred and made available in line with the requirements and protections set out in the UK General Data Protection Regulation, which states that personal data must be:
- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- 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. (see retention schedule)
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller and has Data Protection Officer for the Trust.
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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.
- Use personal data only on secure password-protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password-protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected remembering many memory sticks/cards and other mobile devices cannot be password protected.
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

9. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education to outweigh their risks/disadvantages:

	Staff & other adults			**Pupils**				
Communication Technologies	Allowed	Allowed at certain times	Not Allowed	School Discretion *	Allowed	Allowed in Residence	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x	x			x			
Use of mobile phones in lessons		x						x
Use of mobile phones in social time	x			x		x		
Taking photos on mobile phones / cameras			x					x
Use of other mobile devices e.g. tablets, gaming devices	x					x		
Use of personal email addresses in school, or on school network		x						x
Use of school email for personal emails			x					x

Use of messaging apps		x				x		
Use of social media		x				x		
Use of blogs (school blogs only)		x			x			

**DFE Guidance advises against pupil use of mobile phones in school social time*

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents and carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class or group email addresses may be used at KS1, while pupils at KS2 and above may be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

10. Social Media - Protecting Professional Identity

All schools have a duty of care to provide a 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, cyberbully, discriminate on the grounds of sex, race or 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 limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff in line with the Staff Code of Conduct should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff

- They do not post or communicate disparaging or defamatory statements using social media or otherwise about:
  our employees;
  our governors;
  our learners and their parents/carers;
  our suppliers, agents and contractors
  our Trustees
- Statements that could be construed as being damaging or detrimental to the reputation of the school
- They do not engage in an online discussion on personal matters relating to members of the school community
- They are personally responsible for what they communicate via social media and that what they publish might be read by an audience wider than they intended.
- They must ensure that any social media communication is communicated on their own behalf and does not appear to be linked with the school in any way
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Must not make contact with pupils on social networking sites. Any electronic or text communication should be conducted through the school's communication systems when there is a clear and demonstrable school reason
- Should not have any present pupils or those that have left less than six years ago as "friends", except relatives. However, if there is a legitimate reason for such communication such as involvement with relevant clubs such as Scouts, Youth Club or Football, then this should be declared to the Headteacher and a copy of that organisation's safeguarding policy should be provided

The expectations below apply whether or not the social media is accessed using School facilities and equipment or equipment belonging to staff personally and to the use of social media for both school and personal purposes, whether or not during working hours or otherwise

Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					x
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					x
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					x
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					x
	pornography				x	
	promotion of any kind of discrimination				x	
	threatening behaviour, including promotion of physical violence or mental harm				x	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				x	
Using school systems to run a private business					x	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					x	
Infringing copyright					x	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					x	
Creating or propagating computer viruses or other harmful files					x	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					x	
On-line gaming (educational)					x	
On-line gaming (non-educational)					x	
On-line gambling					x	
On-line shopping / commerce					x	
File sharing					x	
Use of social media					x	
Use of messaging apps			x			
Use of video broadcasting e.g. YouTube			x			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the website (s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

11. Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should 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 (address) of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national/local organisation (as relevant).
- Police involvement and/or action
- If the content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - Incidents of ‘grooming’ behaviour
    - The sending of obscene materials to a child
    - Adult material which potentially breaches the Obscene Publications Act
    - Criminally racist material
    - Other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

12. School Actions and Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows;

CYP	Actions / Sanctions								
Incidents: All incidents will be thoroughly investigated and any of the following sanctions may apply depending on mitigating factors	**Refer to class teacher/ tutor**	**Refer to Department Lead**	**Refer to Headteacher**	**Refer to Police**	**Refer to technical support staff re**	**Inform parents/ carers**	**Removal of network/**	**Warning**	**Further sanction e.g. detention /**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x					
Unauthorised use of non-educational sites during lessons	x								
Unauthorised use of mobile phone / digital camera / other mobile device	x	x	x			x			
Unauthorised use of social media / messaging apps / personal email	x	x	x			x			
Unauthorised downloading or uploading of files	x	x	x				x		
Allowing others to access school network by sharing username and passwords	x	x	x		x			x	
Attempting to access or accessing the school network, using another pupil's account	x	x	x		x				
Attempting to access or accessing the school network, using the account of a member of staff	x	X	x		x	x	x	x	
Corrupting or destroying the data of other users	x	X	x			x	x	x	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	X	x			x	x		
Continued infringements of the above, following previous warnings or sanctions	x	X	x			x	x	x	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	X	x			x		x	
Using proxy sites or other means to subvert the school's filtering system	x	X	x		x	x	x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	X	x		x	x		x	

Deliberately accessing or trying to access offensive or pornographic material	x	X	x		x	x	x	x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	X	x		x	x	x	x	x

Staff	Actions / Sanctions					
Incidents: *All incidents will be thoroughly investigated and any of the following sanctions may apply depending on mitigating factors*	**Refer to line manager**	**Refer to Headteacher**	**Refer to Human Resources**	**Refer to Police**	**Refer to Technical Support Staff for action re filtering etc.**	**Action under disciplinary policy up to and**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x		x
Inappropriate personal use of the internet / social media / personal email	x	x	x			x
Unauthorised downloading or uploading of files	x	x	x	x		x
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x	x	x		x	x
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x	x			x
Deliberate actions to breach data protection or network security rules	x	x	x			x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x	x			x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x			x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils / pupils	x	x	x	x		x
Actions which could compromise the staff member's professional standing	x	x	x			x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x	x			x
Using proxy sites or other means to subvert the school's filtering system	x	x	x			x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x	x		x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x			x
Breaching copyright or licensing regulations	x	x	x			x
Continued infringements of the above, following previous warnings or sanctions	x	x	x			x

13. School Technical Security including cyber security, filtering and passwords

Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place.

Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

The Trust uses LEAD IT services to assist them in providing a complete system and technologies that helps to keep pupils, and staff safe across the Embark family of schools.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. This includes

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Mobile device security and management procedures are in place (where mobile devices are allowed access to school systems)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement
- Remote management tools are used by staff to control workstations and view users' activity
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school system.
- The school infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

14. Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering process to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

The responsibility for the management of the school's filtering process will be held by the Network Manager. They will manage the school filtering and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:
- be logged in change control logs
- be reported to a second responsible person (The Headteacher):
- be reported to and authorised by a second responsible person prior to changes being made

All users have a responsibility to report immediately to the Network Manager any infringements of the school's filtering of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.
Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists .

Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to filtering breaches, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where

personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by the Internet Service Provider (or other filtering service provider)
- The school has provided enhanced/differentiated user-level filtering
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff or the Network Manager. If the request is agreed upon, this action will be recorded and logs of such actions shall be reviewed regularly.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to The Network Manager who will decide whether to make school-level changes (as above).

Monitoring, Audit and Reporting

The appropriateness of any filters and monitoring systems are reviewed by the Trust IT Team and schools will be informed in part, by the risk assessment required by the Prevent Duty.

All Embark schools will have access to a 3-tier filtering solution to provide schools with a comprehensive filtering platform to protect its staff, students, and community regardless of what device is used in school. The solution will also provide the following reports required for the Governance, School Leadership team and DSLs to carry out their duties:

- A number of automated weekly reports will be emailed to DSLs for monitoring review.
- A filtering risk assessment per school for review and sign off each year.
- Full yearly audits performed documenting the filtering systems, testing blocking, keyword detection but ensuring it does not impact teaching and learning. These will be aligned with the new DfE Filtering frameworks.
- Governance report on filtering to ensure governors are able to review and evidence that checks are taking place to review the effectiveness.

No filtering or monitoring solution can offer educational settings 100% protection from exposure to inappropriate or illegal content, so it is important this school demonstrates they have taken all other reasonable precautions.

The school will therefore, monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement

Logs of filtering change controls and of filtering incidents will be made available to:

- The Headteacher
- DSL
- Online Safety Governor
- Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

A DSL in the school will undertake a regular review of filtering systems and will assist and check that technicians in Embark Trust schools comply with the DFE 2023 Standards in Filtering and Monitoring.

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

15. Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks and devices.

- All users will 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 by the DSL.
- All school networks and systems will be protected by secure passwords that are regularly changed
- The “master / administrator” passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place e.g. school safe. Consideration should also be given to using two-factor authentication for such accounts.
- A school should never allow one user to have sole administrator access
- Passwords for new users and replacement passwords for existing users will be allocated by the Network Manager.
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Users will change their passwords at regular intervals – as described in the staff and pupil sections below
- Requests for password changes must be made via the Network Manager

Staff passwords:

- All staff users will be provided with a username and password by the Network Manager who will keep an up-to-date record of users and their usernames.
- Must not include proper names or any other personal information about the user that might be known by others
- The account should be “locked out” following six successive incorrect log-on attempts
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on

- Shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- Should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- Should be changed at least every 90 days
- Should not be re-used for 6 months. Passwords cannot be re-used passwords created by the same user.
- Should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- Should be different for systems used inside and outside of school

Pupil/pupil passwords

- All users at KS2 and above will be provided with a username and password by the Network Manager who will keep an up-to-date record of users and their usernames.
- Users will be required to change their password every term
- Pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regard to the cognitive ability of the children.

Training / Awareness

Members of staff will be made aware of the school's password procedure

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement
- Pupils will be made aware of the school's password policy: in lessons a reminder will be given about the importance of not sharing passwords through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The Network Manager will ensure that full records are kept of:

- User IDs and requests for password changes
- User log-ons
- Security incidents related to this policy

Relevant other school policies:

- Child Protection and Safeguarding Policy
- Behaviour Management/Positive Relationships Policy
- Complaints Policy
- Confidentiality policy
- EMBARK Trust Acceptable Use of the Internet and Electronic Communication
- Anti-Bullying policy
- Data Protection Policy
- Staff Code of Conduct
- NEN Technical guidance:
- Somerset Guidance for schools – this checklist is particularly useful where a school uses external providers for its technical support / security
- Education Act 1996
- Education and Inspections Act 2006

- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990
- Searching Screening and Confiscation Jan 2018

16. National links and resources

- www.thinkuknow.co.uk
- CEOP www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- NCMEC's Take it Down tool https://takeitdown.ncmec.org/

Appendix 1 Pupil acceptable use agreement

Pupil Acceptable Use Policy Agreement for Pupils

Please sign and return to school			
This is how we stay safe when we use IT devices:			
I will ask a teacher or suitable adult if I want to use a device			
I will only use activities that a teacher or suitable adult has told or allowed me to use.			
I will take care of IT devices 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 the screen.			
I know that if I break the rules I might not be allowed to use IT devices and other equipment			
Name of Pupil			
Group / Class			
Signed		**Date**	
As the parent / carer of the above child, I give permission for my son / daughter to have access to the internet and ICT systems at school.			
Signed (Parent / Carer)		**Date**	

Appendix 2 Annual Online Safety School Audit and Risk Assessment Tool

According to Keeping Children Safe in Education, “Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face.”

A free online safety self-review tools for schools can be found on the SWGFL Website or LGFL website

Online Safety Self-Review Tool for Schools | 360safe

Online Safety Audit from LGfL

It is vital that an online safety audit is neither treated as a tickbox exercise, nor viewed as a static report: it should be a living document that reflects the fluid realities of technological change, evolving harms and user behaviours.

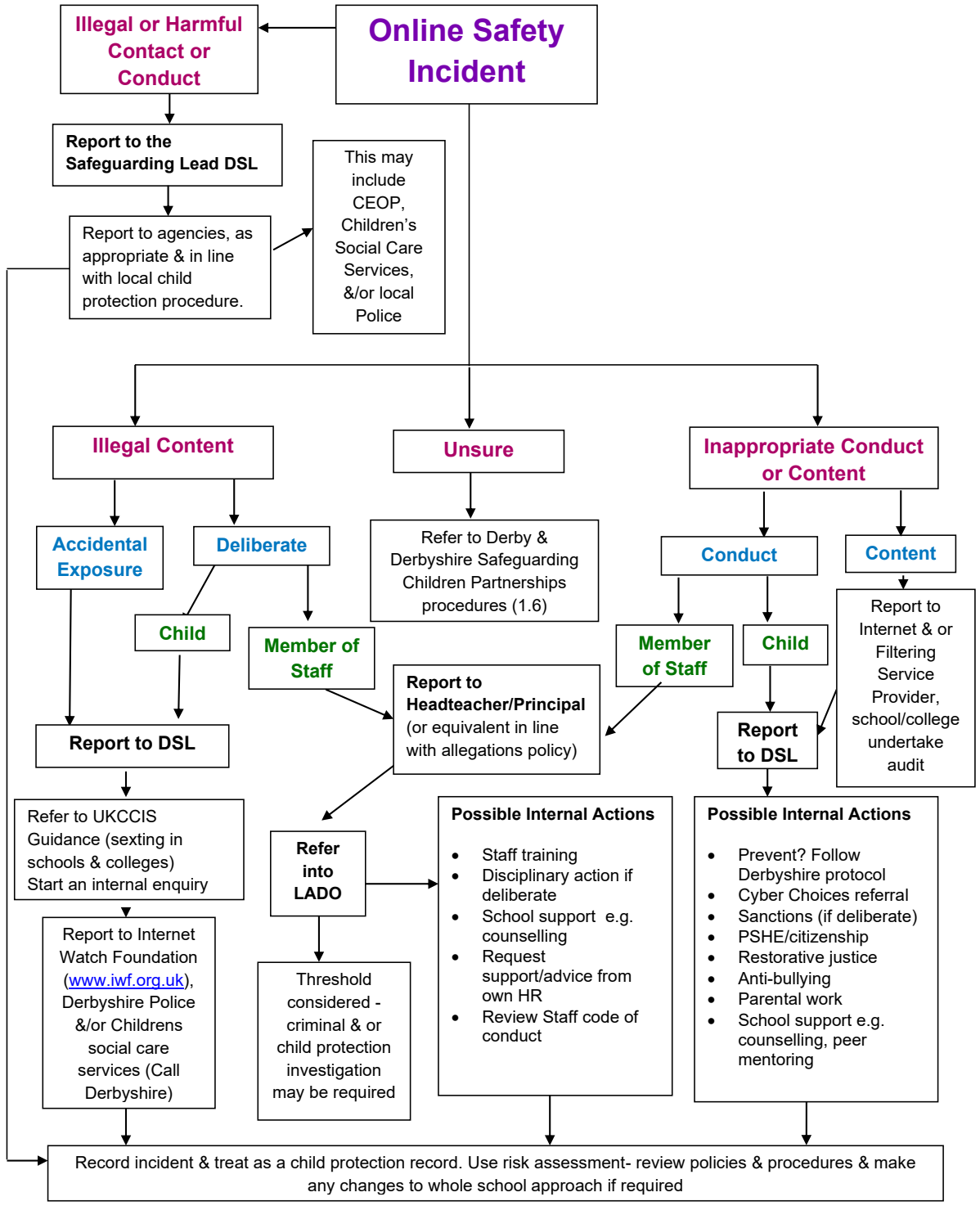
An online safety audit should be carried out by or with the safeguarding team, in recognition that “the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)” (Keeping Children Safe in Education, emphasis added).

UKCIS has published an Online safety in schools and colleges: Questions from the governing board. The questions can be used to gain a basic understanding of the current approach to keeping children safe online; learn how to improve this approach where appropriate; and find out about tools which can be used to improve the approach.

Online safety in schools and colleges: Questions from the Governing Board (2022) (publishing.service.gov.uk)

It has also published an Online Safety Audit Tool which helps mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring.

UKCIS Online Safety Audit for ECTs and ITTs 2022

Appendix 3. Responding to an Online Safety Concern Flow Chart

Responding to an Online Safety Concern