MINDJAM ONLINE SAFETY POLICY

Approved by: Dan Clark, Leo Worsdale

This policy applies to all members of MindJam (including mentors, mentees, parents and carers, and community users) who have access to and are users of digital systems pertaining to MindJam.

Created; February 2022

Reviewed: February 2025

Next Review: February 2026

SCOPE OF THE ONLINE SAFETY POLICY

This Online Safety Policy outlines the commitment of MindJam to safeguard members of our community online in accordance with statutory guidance and best practice following the 4 Cs, which are;

- **Content**
  The content that children and young people see online, which can be harmful, illegal, or inappropriate
- **Contact**
  The risk of harm that children face when interacting with other users online, such as peer pressure or inappropriate advertising
- **Conduct**
  The way people behave online, such as online bullying
- **Commerce**
  The risk from online gambling, phishing, financial scams, and inappropriate advertising

The legal Framework on which this policy is built is listed under the legislative framework.

This Online Safety Policy applies to all members of the MindJam community, including mentors, mentees, parents, carers and guardians, who have access to digital systems pertaining to MindJam.

MindJam will deal with such incidents within this policy and associated behaviour and will, where known, inform parents/carers of inappropriate online safety behaviour that takes place.
This Online Safety Policy has been developed by the MindJam Senior Leadership Team in accordance with other policies of its kind.

CONTENTS

THE MINDJAM ETHOS

We believe that:

- Children and young people should never experience abuse of any kind
- Children should be able to use the internet for education and personal development, but safeguards

need to be in place to ensure they are kept safe at all times.

We recognise that:

• The online world provides everyone with many opportunities; however, it can also present risks and challenges

• We have a duty to ensure that all children, young people, and adults involved in our organisation are protected from potential harm online

• We have a responsibility to help keep children and young people safe online, whether or not they are using MindJam's network and devices

• All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse

• Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

SCHEDULE FOR DEVELOPMENT, MONITORING AND REVIEW

This Online Safety Policy was approved by	10/02/2022

MindJam on:	
The implementation of this Online Safety Policy will be monitored by:	The MindJam Senior Leadership Team
Monitoring will take place at regular intervals:	Annually in February
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	February 2026
Should serious online safety incidents take place, the following persons should be informed:	Vikki Hearst - safeguarding@mindjam.org.uk Dan Clark - danclark@mindjam.org.uk

MindJam will monitor the impact of the Online Safety Policy by using logs of reported incidents, internal monitoring of mentor activity where necessary and a concern has been raised, by using CPOMS and contacting parents/guardians in case of incidents.

POLICY AND LEADERSHIP

Responsibilities

To ensure the online safeguarding of members of the MindJam community it is important that all members of the community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate or unsafe online behaviours, concerns, and misuse as soon as they become apparent. While this will be a team effort across MindJam, the following sections outline the safety roles and responsibilities of those within MindJam.

The Founder/Owner and Senior Leadership Team

- The senior members of MindJam (Including all members of the Senior Leadership Team and the Founder/Owner of MindJam) have a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding
- The Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- The Senior Leadership Team are responsible for ensuring that all members of the Senior Leadership Team and all MindJam mentors carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant

Mentors

Mentors are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current MindJam Online Safety Policy and practices
- They understand that online safety is a core part of safeguarding
- Mentors use their own equipment responsibly and in accordance with MindJam policies.
- They immediately report any suspected misuse or problem to a member of the Senior Leadership Team for investigation/action, in line with MindJam safeguarding procedures
- All digital communications with mentees and their parents/carers should be on a professional level, any communication outside of session must be approved with parents beforehand. Mentor must be able to provide proof of permission should it be requested
- Session notes are kept securely and not shared with anyone other than the parents/carers and funding parties.
- Online safety issues are embedded in all aspects of MindJam activity
- Where mentees use live-streaming or video-conferencing, mentors must have full regard to national safeguarding guidance and MindJam safeguarding policies
- Have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- They model safe, responsible, and professional online behaviours in their own use of technology, including in their use of social media

Parents and Carers

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

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

- Publishing their Online Safety Policy on MindJam's website
- Seeking their permissions concerning digital images, recording, contact outside of sessions, and any other Online Safety concerns
- Answering any concerns parents raise regarding online safety via email, message, call or MindJam's social media. Including signposting to further online safety info

Parents and carers will be encouraged to support MindJam in:

- Reinforcing the online safety messages provided to mentees
- The safe use of their children's personal devices
- The safe use of their children's online accounts

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of MindJam i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of MindJam and its wider community.

POLICY

Online Safety Policy

The DfE guidance "Keeping Children Safe in Education" states: "Online safety and the school or college's approach to it should be reflected in the child protection policy"

While MindJam is neither a school nor a college, we as a company work with schools and Local Authorities as well as school age children and young people, therefore our policies and protocols, such as our use of CPOMS, is based on those of Educational bodies.

THE PURPOSE OF THIS POLICY STATEMENT

The MindJam Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, communication, and recreation
- Allocates responsibilities for the delivery of the policy
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- Establishes guidance for mentors in how they should use digital technologies responsibly, protecting themselves and MindJam as a company, and how they should use this understanding to help safeguard mentees in the digital world
- Describes how MindJam will help prepare and support mentees to be safe and responsible users of online technologies
- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents
- Is made available to mentors at induction and through normal communication channels such as Discord, Email, and on their MindJam Drive.
- Is published on the MindJam website

ACCEPTABLE USE

MindJam has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Any illegal activity for example: • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to MindJam networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant					X

	permission) *N.B. MindJam will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways*					

When using communication technologies, MindJam considers the following as good practice:

• When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by MindJam.
• All communication tools should be approved by parents/carers. Tools sanctioned by MindJam include (but are not limited to) Google Meets, Zoom, Teams, Discord, Whatsapp, Xbox Live and PlayStation Network.
• Any digital communication between staff and learners or parents/carers (e-mail, social media, video conferencing, phone call etc.) must be professional in tone and content

- Contacting mentees outside of session must be done so only with permission from parent/carer, mentor should be able to produce evidence of permission if requested
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of MindJam and its community
- Users should immediately report to a nominated person – in accordance with the Online Safety Policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Relevant policies and permissions should be followed when posting information online e.g., school website and social media.
- Any recording or posting (to social media or MindJam's website) of mentees or their work must only be posted with the permission of the mentee and their primary parent/carer.
- Mentees may choose where they are located to do the session. This may include their own bedroom. MindJam will not refuse this request for engagement reasons, provided we have permission from the parent/carers.
- Mentees may also choose when the sessions take place. Again, this is for engagement purposes and may be before 8am or after 5pm.

REPORTING AND RESPONDING

MindJam will take all reasonable precautions to ensure online safety for all MindJam users (both mentors and mentees) but recognises that incidents may occur internally within sessions, and externally (with

impact on mentees) which may need intervention. MindJam will ensure:

- That there are clear reporting routes which are understood and followed by all members of the MindJam community which are consistent with MindJam's safeguarding procedures.
- All members of the MindJam community will be made aware of the need to report online safety issues/incidents
- Reports will be dealt with as soon as practically possible once they are received
- The Senior Leadership Team have appropriate skills and training to deal with online safety risks
- All mentors will undergo annual Online Safeguarding training
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through MindJam safeguarding procedures
- Any concern about staff misuse will be reported to the Owner/Founder (Dan Clark) and Head of Safeguarding (Vikki Hearst), unless the concern involves the Owner/Founder or Head of Safeguarding, in which case the complaint is referred to the person who is not involved. Should a concern ever arise involving both members of MindJam the complaint should be raised with the Senior Leadership Team who will escalate accordingly.
- Where there is no suspected illegal activity, but a complaint or concern is raised, mentor's accounts may be checked using the following procedures:
    - One or more senior members of MindJam should be involved in this process to protect the interests of both parties. This is vital to protect individuals if accusations are reported
    - Conduct the procedure using an assigned device and only this device for the duration of the search
    - Record the URL or application that contains 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/device being used for investigation. These may be printed, signed, and attached as evidence
    - Once this has been completed and fully investigated the group forming the investigation 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
        - Police involvement and/or action

- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident, or support through our Mental Health First Aiders (Abbie Wilson & Max McGrorty)
- Incidents should be logged on CPOMS where a mentee is concerned, and on the MindJam database where mentors are involved in the perpetration
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Report Harmful Content; CEOP Safety Centre

- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- Learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - The Senior Leadership Team for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - Staff, through regular briefings
    - Parents/carers, through social media, website, and newsletters

MINDJAM ACTIONS

It is more likely that MindJam 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 MindJam 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:

RESPONDING TO MENTEE ACTIONS

Incidents	Note in session report	Notify member of SLT	Inform parent/guardian	Report through CPOMS	Notify Police
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section regarding illegal activity)	X	X	X	X	X
Using another MindJam user's account (mentor or mentee) or allowing others to access MindJam network by sharing username and password	X	X	X		
Sending an email, text, or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		
Accidentally accessing offensive or pornographic material in session and failing to report to mentor	X	X	X		
Deliberately accessing offensive or pornographic material in session and failing to report to mentor	X	X	X		
Unauthorised use of digital devices (i.e., taking pictures or screenshots of mentor without permission, recording without permission) as a single incident	X		X		
Unauthorised use of digital devices (i.e., taking pictures or	X	X	X		

screenshots of mentor without permission, recording without permission) as a repeated incident					

*In the rare instance that there are continued infringements of the above, following previous sanctions to no effect, MindJam will look to remove mentee from their register.
In the instance that the mentee's actions are aimed at or affecting one mentor in particular, MindJam reserves the right to swap the mentee to a new mentor.*

RESPONDING TO STAFF ACTIONS

Incidents	Refer to Senior Lead Team	Refer to Owner/Founder Dan Clark and/or Senior Management & Lead Mentor Leo Worsdale	Refer to police	Issue warning	Issue written warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section regarding illegal activity)		X	X				X
Deliberate actions to breach data protection or network security rules		X					X
Corrupting or destroying the data of other mentors or causing deliberate damage to hardware or software		X					X
Unauthorised downloading or	X	X		X			

uploading of files or file sharing (First instance)							
Unauthorised downloading or uploading of files or file sharing (Further instance)	X	X			X		X
Allowing others to access MindJam by sharing username and passwords or attempting to access the MindJam network using another mentor's account		X				X	X
Sending an email, text, or message that is regarded as offensive, harassment or of a bullying nature		X				X	X
Inappropriate personal use of the digital technologies e.g., social media/personal email				X			
Careless use of personal data, e.g., displaying, holding or transferring data in an insecure manner		X				X	
Actions which could compromise the staff member's professional standing.		X		X	X		
Actions which would bring MindJam into disrepute or breach the integrity or the ethos of MindJam		X			X	X	X

Failing to report incidents whether caused by deliberate or accidental actions		X			X	X	
Continued infringements of the above, following previous warnings or sanctions		X					X

ONLINE SAFETY EDUCATION FOR MENTEES

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.
Online safety should be a focus throughout every MindJam session and mentors should reinforce online safety as part of their interactions with mentees.
This may be provided in the following ways:

- Online safety in sessions matched to need; are age and ability-related
- Mentee needs and progress regarding online use and safety assessed across the duration of sessions
- Mentors should act as good role models in their use of digital technologies, the internet, and devices
- Suitability of games, applications, websites etc., should be checked with parents where age or temperament may need consideration i.e., in playing higher rated games, or before downloading Discord

FAMILIES

Some 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 online behaviours. Parents may underestimate how children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

MindJam will seek to provide information and awareness to parents and carers through:

- Communication, raising awareness and engagement on safety issues through the MindJam social media.

- Access to online safety advice on the MindJam website with reference to the relevant websites/publications.
- Mentees – who may pass on to their parents the online safety messages they have learned through sessions and their mentors.
- Mentors – who may advise parents/guardians where needed or requested.

TECHNOLOGY

MindJam is responsible for ensuring that MindJam infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. MindJam should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

TECHNICAL SECURITY

MindJam technical systems will be managed in ways that ensure that MindJam meets recommended requirements.

- There will be regular reviews and audits of the safety and security of MindJam's servers and databases
- There are back-up routines, including the copy of data stored in the cloud to help prevent loss of data from ransomware attacks
- All mentors have the responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security to SLT
- The master account passwords for the MindJam systems and users are kept in a secure place.
- Passwords should be long and unique, particularly avoiding passwords already in use or pertaining to mentors' personal passwords outside MindJam

DIGITAL AND VIDEO IMAGES

Mentors, parents/carers and mentees need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.
MindJam 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, mentors will inform and educate mentees about the risks associated with the taking, use, sharing, publication and distribution of images.
- Mentees must not take, use, share, publish or distribute images of others or their mentors

without permission

- Mentees' full names will not be used anywhere on MindJam's social media or website, particularly in association with any images or photographs
- Written permission from parents/carers will be obtained before photographs or videos of learner's work are published on MindJam's social media or website
- Parents/carers will be informed of the purposes for the use of the images, how they will be stored and for how long
- Images will be securely stored

ONLINE PUBLISHING

MindJam communicates with parents/carers and promotes MindJam through:

- Public facing website
- Social media
- Online newsletter (Quarterly)

MindJam's website and social media is managed by Adam Rowe, Chief Marketing Officer (CMO). MindJam ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, and the publication of personal information – ensuring that there is least risk to members of the MindJam community, through such publications. Where a mentee's work, images, videos, games, or creations are published, their identities are protected, and full names are not published.

DATA PROTECTION

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

MindJam:

- Has a data protection policy
- Implements the data protection principles and can demonstrate that it does so
- Has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest
- Has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why, and which member of staff has responsibility for managing it
- Will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for
- Data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents/carers to check primary contact

information at suitable intervals

- Provides mentors, mentees, and parents/carers with information about how MindJam looks after their data and what their rights are in a clear Privacy Notice
- Has procedures in place to deal with the individual rights of the data subject
- Carries out Data Protection Impact Assessments where necessary
- Has undertaken appropriate due diligence and has data protection compliant contracts in place
- Understands how to share data lawfully and safely with other relevant data controllers
- Has clear and understood policies and routines for the deletion and disposal of data
- Reports any relevant breaches to the Information Commissioner within 72 hours of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- Has a Freedom of Information Policy which sets out how it will deal with FOI requests
- Provides data protection training for all staff at induction and appropriate refresher training thereafter.

When personal data is stored on any mobile device or removable media the:

- Data will be password protected and encrypted
- Device will be password protected
- Device will be protected by up-to-date anti-virus software
- Data will be securely deleted from the device, in line with MindJam policy once it has been transferred or its use is complete

Mentors must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse
- Can recognise a possible breach, understand the need for urgency and know who to report it to within MindJam
- Can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in MindJam
- Transfer data using encryption, a secure email account, and secure password protected devices

OUTCOMES

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs, behaviour/bullying reports, surveys of staff, and is reported to relevant groups:
• There is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
• There are well-established routes to regularly report patterns of online safety incidents and outcomes to

MindJam leadership

• Parents/carers are informed of patterns of online safety incidents as part of MindJam's online safety awareness raising

• Online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate

LEGISLATION

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England/Northern Ireland/Scotland/Wales. Summaries of the key legislation and guidance are available on:

• online abuse **learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse**

• bullying **learning.nspcc.org.uk/child-abuse-and-neglect/bullying**

• child protection **learning.nspcc.org.uk/child-protection-system**

MindJam should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Online Safety Act 2023

This Act provides for a new regulatory framework which has the general purpose of making the use of internet services safer for individuals. The purpose of this Act is to:

- imposes duties which, in broad terms, require providers of services regulated by this Act to identify, mitigate and manage the risks of harm (including risks which particularly affect individuals with a certain characteristic) from illegal content and activity, and content and activity that is harmful to children
- Confers new functions and powers on the regulator, OFCOM
- Duties imposed on providers by this Act seek to secure (among other things) that services are safe by design, and are designed and operated in such a way that a higher standard of protection is provided for children than for adults, users' rights to freedom of expression and privacy are protected, and transparency and accountability are provided in relation to those services

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

The National Crime Agency website includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

This protects the rights and privacy of an individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support staff.
- MindJam reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered TradeMarks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trademarks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which they know or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against them is guilty of an offence if they know or ought to know that their course of conduct will cause the other to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Protection of Freedoms Act 2012
Requires permission from a parent/carer to use Biometric systems

Serious Crime Act 2015

Introduced a new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

RELATED POLICIES AND PROCEDURES

This policy statement should be read alongside our organisational policies and procedures, including:

- KCSIE
- Child protection
- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff
- Code of conduct for staff
- Anti-bullying policy and procedures
- Photography and image sharing guidance

LINKS

Child Exploitation and Online Protection command: CEOP is a law enforcement agency which aims to keep children and young people safe from sexual exploitation and abuse. Online sexual abuse can be reported on their website and a report made to one of its Child Protection Advisors

The NSPCC provides a helpline for professionals at 0808 800 5000 and help@nspcc.org.uk. The helpline provides expert advice and support

Support from specialist sexual violence sector organisations such as Rape Crisis or The Survivors Trust
The Anti-Bullying Alliance has developed guidance about Sexual and sexist bullying.

The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. The helpline provides expert advice and support for staff with regard to online safety issues

The Internet Watch Foundation: If the incident/report involves sexual images or videos that have been made and circulated online, the victim can be supported to get the images removed by the Internet Watch Foundation (IWF)

Childline/IWF Report Remove is a free tool that allows children to report nude or sexual images and/or videos of themselves that they think might have been shared online

UKCIS Sharing nudes and semi-nudes advice: Advice for education settings working with children and young people on responding to reports of children sharing non-consensual nude and semi-nude images and/or videos (also known as sexting and youth produced sexual imagery).

Thinkuknow from NCA-CEOP provides support for the children's workforce, parents and carers on staying safe online

The Lucy Faithfull Foundation

Marie Collins Foundation

NSPCC National Clinical and Assessment Service (NCATS)

Project deSHAME | Childnet

CONTACT DETAILS

MindJam Point of Contact:
Dan Clark
01522 462978

NSPCC Helpline
0808 800 5000

We are committed to reviewing our policy and good practice annually. This policy was last reviewed: February 2025.

Dan Clark
CEO / Founder MindJam Ltd

More ways to help you protect children:

Complete NSPCC's online course Keeping children safe online.
Sign up to NSPCC's weekly current awareness email newsletter nspcc.org.uk/caspar
Visit nspcc.org.uk/vcs for more information and resources for voluntary and community organisations.