NORTHWEST
LONDON JEWISH DAY SCHOOL
Striving to achieve excellence for all

E-Safety Policy

Date: September 2025
Review Date: September 2026

E-Safety and Internet Usage
E-safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's E-safety policy will operate in conjunction with other policies including:
- Safeguarding and Child Protection Policy
- GDPR Policy
- Behaviour Policy
- Anti-bullying Policy
- PSHE/SRE policy
- Wellbeing Policy
- AI Policy

Safeguarding Lead	Miss Judith Caplan (Headteacher)
Deputy Safeguarding Leads	Rabbi Ronen Broder
Child Protection Teacher	Mrs Amanda Shoota
Deputy Child Protection Teachers	Miss Judith Caplan / Mrs Madeleine Bendell
E-Safety Lead	Miss Judith Caplan
IT Coordinator	Mrs Camilla Isaac
Safeguarding Governor	Mrs Sheila Taylor

Background - Why Is Internet Use Important?
The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use and Independent Jewish Day School (NWLJDS) has a duty to provide pupils with quality internet access. Many pupils will access the internet outside school and will need to learn how to evaluate online information and to take care of their own safety and security.

How Does Internet Use Benefit Education?
Benefits of using the internet in education include:
- access to world-wide educational resources including museums, libraries and art galleries
- rapid and cost effective worldwide communication
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between pupils worldwide
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of
- networks and automatic system updates
- exchange of curriculum and administration data with the Local Authority
- access to learning wherever and whenever convenient
- greatly increased skills in English and digital Literacy

How Can Internet Use Enhance Learning?

- The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of our pupils
- Children will be taught what internet use is acceptable and what is not and given clear objectives for internet use
- Internet access will be planned to enrich and extend learning activities
- Staff will guide pupils in online activities that will support learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

Good Habits

E safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of E-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the provider including the effective management of content filtering.
- National Education Network standards and specifications.

ROLES AND RESPONSIBILITIES

Designated Safeguarding Lead

- has overall responsibility for e-safety in the school
- is responsible for establishing and reviewing the school e-safety policies/documents along with the Headteacher
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- The designated safeguarding lead should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:
  - sharing of personal data
  - access to illegal/inappropriate materials
  - inappropriate online contact with adults/strangers
  - potential or actual incidents of grooming
  - cyberbullying

(N.B. It is important to emphasise that these are child protection issues, not technical issues. The technology provides additional means for child protection issues to develop).

Headteacher and DSL:

The Headteacher is responsible for:

- the safety (including e-safety) of all members of the school community, though the day-to-day responsibility for e-safety will be delegated to the Designated Safeguarding Lead (DSL)
- The DSL is responsible for ensuring that staff receive suitable training to enable them to follow and enforce his policy throughout the school
- liaises with school technical staff
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides advice for staff
- provides updates for parents on important e-safety issues
- keeps up to date with e-safety technical information and advice in order to carry out their role effectively and inform and update others as relevant once a term
- ensures that all users of the school computing systems have signed and agreed to the Staff Acceptable Use of Computing Agreement.

Technical Staff:
The technical staff are responsible for ensuring:
- liaison with school
- day-to-day responsibility for protecting against e-safety issues
- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy
- that web filtering is updated on a regular basis
- that network and endpoint security systems are implemented and updated

Teaching and support staff:
The teaching and support staff are responsible for ensuring that:
- they have an up-to-date awareness of e-safety matters and of the school's e-safety policy and practices in an annual e-safety inset day
- they have read, understood and signed the Staff Acceptable Use of Computing Agreement
- all digital communications with children/parents/carers and staff should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- children and parents understand e-safety
- children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- staff monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- staff check websites and online videos before use in lessons, pre-loading videos to avoid adverts
- in lessons where internet use is pre-planned, children 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.

Children
The children:
- 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 cyberbullying
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-safety Policy covers their actions out of school, if related to their attendance at the school.

Parents/carers:
Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will help parents understand these issues through parents' evenings, newsletters, the website and further literature. Parents and carers are expected to act as a positive role model and will use social media responsibly in respect of all matters relating to the school. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines regarding:

- the appropriate use of digital and video images taken at school events
- their children's personal devices not being brought into school

Volunteers and peripatetic teachers:
Volunteers and peripatetic teachers who access school systems as part of the wider school provision will be expected to sign a Staff Acceptable Use of Computing Agreement before being provided with restricted access to school computing.

Education and training – staff/volunteers:
It is essential that all staff receive e-safety training and understand their responsibilities, Training will be offered as follows:
- Formal e-safety training will be made available to staff either alone or as part of wider safeguarding training
- All new staff should receive e-safety training as part of their induction programme
- This e-safety policy and its updates will be presented to and discussed by staff in staff/team meetings/inset days.
- The DSL will provide advice/guidance/training to individuals as required.
- Participating in events/campaigns such as Safer Internet Day

ICT-BASED FORMS OF ABUSE

Information and communication technology(ICT)-based forms of child physical, sexual and emotional abuse can include bullying via mobile telephones or online (internet) with verbal and visual messages.

This annexe focuses on child sexual abuse and bullying. However, the procedure will be followed in other instances of ICT-based abuse e.g. physical abuse (such as, pupils being constrained to fight each other or filmed being assaulted).

Recognition and response:
The impact on a child of ICT-based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse.

Recognition and response is recognising a situation where a child is suffering, or is likely to suffer, a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family.

All adults (volunteers and staff) will be alerted to the possibility that:
a child may already have been/is being abused and the images distributed on the internet or by mobile telephone
an adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images
an adult or older child may be viewing and downloading child sexual abuse images.

Chat-room grooming and offline abuse:
Our staff will need to be continually alert to any suspicious activity involving computers and the internet. Grooming of pupils online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting

a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

E-safety:
The Child Exploitation and Online Protection Centre (CEOP) brings together law enforcement officers, specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24-hour online facility for reporting instances of online child sexual abuse. The main concern for teachers is the safe and effective supervision of pupils using the internet in school. However, many pupils now use the internet at home for homework and socialising, therefore the staff will need to help the parents understand the positive ways in which the internet can be used, but also some of the associated risks.

Child-on-Child Abuse – (read in line with the Safeguarding and Child Protection Policy):
All staff should recognise that children are capable of abusing their peers. This can include (but is not limited to) bullying including cyberbullying.

- Child-on-Child sexual abuse is sexual abuse that happens between children.
- It can happen between any number of children and can affect any age group.
- It is important that staff report any concerns as soon as possible.
- The school recognises that even if there are no reported cases of Child-on-Child abuse, such abuse may still be taking place and is simply not being reported.
- Children can experience Child-on-Child abuse in a wide range of settings, including at school, at home or in someone else's home, in public spaces and online.

Cyber-bullying:
"Cyber-bullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly over time against a victim who cannot easily defend him or herself."

We recognise that the advent of cyber-bullying adds a new and worrying dimension to the problem of bullying as there no safe haven for the person being bullied. Unlike other forms of bullying, cyber-bullying can follow pupils and young people into their private spaces and outside school hours. Cyber-bullies can communicate their messages to a wide audience with remarkable speed, and can often remain unidentifiable and unseen. ICT may be used to send threatening pictures or messages to others.

Seven categories of cyber-bullying have been identified.
- Text message bullying involves sending unwelcome texts that are threatening or cause discomfort.
- Picture/video-clip bullying via mobile phone cameras is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks.
- Phone call bullying via mobile phone uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified.
- Email bullying uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- Online grooming, chat room and social networking site abuse involves sending menacing or upsetting responses to pupils or young people.
- Bullying through instant messaging (IM) is an internet-based form of bullying where pupils and young people are sent unpleasant messages as they conduct real-time conversations online.

- Bullying via websites includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

Because of the anonymity that new communications technologies offer, anyone with a mobile phone or internet connection can be a target for cyberbullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips sent by mobile phone. Most cyber-bullying is done by pupils in the same class or year group. Although it leaves no visible scars, cyber-bullying of all types can be extremely destructive.

Staff Training:
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. We must demonstrate that we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks.

E-Safety training takes place for all stake holders annually and below sets out what is in place:

STAKEHOLDER	TRAINING	WHEN
Headteacher / DSL	National Online Safety certified Level 3 certificate in Online Safety for DSLs	Annually
Deputy DSL	National Online Safety certified Level 3 certificate in Online Safety for DSLs	Annually
Staff	Termly updates National Online Safety certificate in Online Safety ECP training	Termly Annually Annually
Governors	Termly / annual updates at Governor Meetings National Online Safety certificate in Online Safety	Termly / annually Annually
Children	Regular e-safety lessons in class, as part of Computing curriculum ECP training E-safety lessons	Termly Annually Termly
Parents	Online safety course, either via National Online Safety or via ECP training	Annually

Children have at least 3 training sessions during an academic year. One takes place each term. Staff use a range of resources (see below for a list but this is not exhausted):

- https://www.youtube.com/watch?v=-nMUbHuffO8 **Reception – Year 3**
- https://www.youtube.com/watch?v=HxySrSbSY7o **Key Stage 2**
- https://www.thinkuknow.co.uk/parents/articles/band-runner/ **Key stage 2**
- **interactive game**

These are more for EYFS and KS1
- http://hectorsworld.netsafe.org.nz/teachers/lesson-plans-and-resources/
- **Hector's World resources and lesson plans**
- https://www.youtube.com/watch?v=uRkpf0bk3P4 **video Hector's world 1**

- https://www.youtube.com/watch?v=XUAXS3P9sDE **video Hector's World 2**
- https://www.youtube.com/watch?v=6cibv8dx5JM **Hector's world – Keeping your personal information safe - Episode 3**

Training includes learning about CEOP (Think You Know), and how to apply this should children, or adults, see anything concerning online - **https://www.thinkuknow.co.uk/**

Use of digital and video images:
The school will inform and educate staff, children and visitors about the risks and will implement procedures to reduce the likelihood of the potential for abuse.

- When using digital images, staff will inform and educate children 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.
- Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, parents/carers should not share or make the images/video publicly available on social networking sites, nor should parents/carers make comments on any activities involving other children on social media.
- 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 must only be taken on school equipment
- Care will be taken when taking digital/video images that children are appropriately dressed (i.e. fully clothed) and are not participating in activities that might bring the individuals or the school into disrepute.
- Care will be taken not to publish any images with personal information on display, i.e. names or other background images unless permission from parents is given.
- Photographs taken will not present any risk to the security of the school.
- Photographs published on the website or elsewhere that include children will be selected carefully and will comply with the consent form signed by parents at the start of each academic year
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data protection:
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

See the GDPR Policy for more details.

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

- The official school email service is from the school office, which is regarded as safe and secure and is monitored

- Staff are aware that email communications may be monitored.
- Users must immediately report, to the E-Safety Teacher, 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 parents/carers (email, chat, etc) must be professional in tone and content
- Personal email addresses, text messaging or social media must not be used for these communications
- Children should be taught about e-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

Social media - Protecting professional identity

All schools have a duty of care to provide a safe learning environment for children and staff. Staff members who harass, cyberbully, discriminate on the grounds of age, disability, gender, gender reassignment, religion or belief, race, sexuality, marital status or maternity or who defame a third party may render the school liable to the injured party.

Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to children, staff and the school through limiting access to personal information:

- training to include acceptable use, social media risks, checking of settings, data protection, and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk.

School staff should ensure that:

- other than on the school social media accounts and school website, no reference should be made on social media to students/children, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Dangers to Consider:

Some of the danger's children may face include:

- Access to illegal, harmful or inappropriate images or other content
- Exposure to misinformation, disinformation and conspiracy theories as safeguarding harms
- Unauthorised 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
- Cyberbullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files

- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Reporting:

- We take all concerns seriously.
- All online concerns are reported to the E-Safety lead and followed up.
- Where there are Child Protection / Safeguarding concerns, the DSL are informed.
- Parents are also informed of a concern so that we work in collaboration to keep children safe on-line.
- 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 – see the Behaviour Policy.

Filtering and Monitoring:

It is recognised by North West London Jewish Day School that the use of technology presents challenges and risks to children and adults both inside and outside of school. As a school we will empower, protect and educate the community in their use of technology and establish mechanisms to identify, intervene in, and escalate any incident where appropriate. The school sees technology and its use permeating all aspects of school. Our integrated approach to online safety is set out in detail in:

- The online safety policy
- Remote learning policy
- behaviour policy
- Threaded through other policies, including policies for the curriculum, such as computing

The school identifies that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk as set out in KCSIE:

- **content**: being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views misinformation, disinformation and conspiracy theories;
- **contact**: being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group.

Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met. This is done by identifying and assigning:

- a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met

- the roles and responsibilities of staff and third parties, for example, external service providers
- The SLT are responsible for:
    - procuring filtering and monitoring systems
    - documenting decisions on what is blocked or allowed and why
    - reviewing the effectiveness of your provision
    - overseeing reports
- They are also responsible for making sure that all staff:
    - understand their role
    - are appropriately trained
    - follow policies, processes and procedures
    - act on reports and concerns
- Senior leaders work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.
- Governors and will review the standards and discuss with IT staff and service providers what more needs to be done to support our school in meeting this standard.

North West London Jewish Day School uses a wide range of technology. This includes: computers, laptops, tablets, Chromebooks, the internet, our learning platform, intranet, email systems, messaging systems and other digital devices and systems. All school owned devices and systems will be used in accordance with our acceptable use policies and with school's appropriate safety and security measures in place. All devices owned by staff, pupils and visitors will also be used in accordance with our acceptable use policies and the appropriate safety and security measures.

North West London Jewish Day School recognises the specific risks that can be posed by mobile technology, including mobile phones and cameras. In accordance with KCSIE 2025 and EYFS 2021 has appropriate policies in place that are shared and understood by all members of the community. Further information regarding the specific approaches relating to this can be found in our online safety and acceptable use and image use policies which can be found on the website or via the school office.

North West London Jewish Day School do all we reasonably can to limit children's exposure to online risks through our school IT systems and will ensure that appropriate filtering and monitoring systems are in place and that these meet the DfE standards for filtering and monitoring (March 2023) these are:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs

To ensure we meet the standards for filtering and monitoring, we will:

- consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks
- be informed in part, by the risk assessment required by the Prevent Duty
- ensure the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified

- inform all users that use of our systems can be monitored, and that monitoring will be in line with data protection, human rights and privacy legislation.
- require pupils, staff and visitors if they discover unsuitable sites or material,

To follow the school procedures: such as:

- turn off screen
- report the concern immediately to a member of staff
- report the URL of the site to technical staff/services
- record and report to the DSL and appropriate technical staff, any filtering breaches or concerns identified through our monitoring approaches. Amend as appropriate.
- immediately report any access to material believed to be illegal to the appropriate agencies, such as the Internet Watch Foundation and the Police.
- ensure that in implementing appropriate filtering and monitoring - "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding
- regularly check (should not time scales/approach - termly or monthly – will depend on the school approach) on the effectiveness of the filtering and monitoring systems
- review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

North West London Jewish Day School acknowledges that whilst filtering and monitoring is an important part of school online safety responsibilities, it is only one part of our approach to online safety a full list of strategies and how keeping safe is taught can be found in the online safety policy.

- Pupils will use appropriate search tools, apps and online resources as identified following an informed risk assessment.
- Pupils' internet use will be supervised by staff according to their age and ability.
- Pupils will be directed to use age-appropriate online resources and tools by staff.

North West London Jewish Day School will ensure a comprehensive whole school curriculum response is in place to enable all learners to learn about and manage online risks effectively as part of providing a broad and balanced curriculum.

North West London Jewish Day School will build a partnership approach to online safety and will support parents/carers to become aware and alert by: online safety training, emails, online safety leaflet, school newsletter.

North West London Jewish Day School will ensure that online safety training for all staff is integrated, aligned and considered as part of our overarching safeguarding approach. This will include amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

The DSL will respond to online safety concerns in line with the child protection and other associated policies such as child-on-child abuse and behaviour.

Internal sanctions and/or support will be implemented as appropriate.

Where necessary, concerns will be escalated and reported to relevant partner agencies in line with local policies and procedures.

Staff will need to complete a request for certain website uses - the template can be found in the appendix of this policy policy.

North West London Jewish Day School Schools. will carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face.

Illegal incidents:

- If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the DSL immediately.
- If the incident concerns a member of staff, it should be reported to the Head.
- In the event of suspicion, all steps in this procedure should be followed by the Safeguarding lead:
    - Have more than one senior member of staff/volunteer involved in this process to investigate: this is vital to protect individuals if accusations are subsequently reported.
    - Conduct the procedure using a designated computer that will not be used by children 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.
    - Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern.
    - It may also be necessary to record and store screenshots of the content on the machine being used for investigation.
    - These may be printed, signed and attached to the reporting log (appendix 1)
    - Once this has been completed and fully investigated, the investigation 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 LADO
    - Police involvement and/or action.
- If content being reviewed includes images of child abuse 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 or other criminal conduct, activity or materials
- 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.

Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents / carers may be familiar with generative chatbots such as: Chat GPT and Google Gemini.

North West London Jewish Day School recognises that AI has many uses, including enhancing teaching and learning, and in helping to protect and safeguard pupils. However, AI may also have the potential to facilitate abuse (e.g. bullying and grooming) and/or expose

pupils to harmful content. For example, in the form of “deepfakes”, where AI is used to create images, audio or video hoaxes that look real.

North West London Jewish Day School will treat any use of AI to access harmful content or bully pupils in line with this policy and our anti-bullying policy, behaviour policy and Acceptable Use of ICT agreement.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out risk assessments for any new AI tool being used by the school. Our school’s requirements for filtering and monitoring also apply to the use of AI, in line with Keeping Children Safe in Education (KCSIE 2025) / DfE Generative AI: product safety expectations.

Should there be any concerns relating to AI — for example where indecent images have been shared that are AI-generated — staff will immediately notify the DSL and E-Safety Lead.

Additionally:

- Any AI tools procured or used must be assessed to ensure compliance with the DfE’s generative AI product safety expectations (e.g. capacity to prevent access to harmful content, maintain logs, be secure against misuse).
- Where AI tools are used in curriculum or assessments, a human oversight / moderation procedure must be in place so that outputs can be checked by staff before pupils view / submit them.
- The use of AI by pupils (for e.g. homework, writing, research) should be governed by clear expectations outlined in the Acceptable Use / ICT policy, including honesty, attribution and integrity.
- Professional development and training for staff should include awareness of AI-related safeguarding risks (e.g. deepfakes, AI-enabled grooming, bias or harmful content).

This policy is reviewed annually.

Signed: Miss Judith Caplan (Headteacher)
Dated: September 2025

Appendix 1: E-Safety Reporting Log (this is held by the E-Safety Lead)

E-Safety Reporting Log

Date	Time	Incident	Action Taken		Incident reported by	Signature of staff	Parent informed (Date and time)
			What?	By Whom?			

NORTHWEST
LONDON JEWISH DAY SCHOOL
Striving to achieve excellence for all

Staff request form template to unblock a specific website(s)

Staff name:

Website title and URL/link:

Year group you want the website unblocked for (if applicable):

Reason why you want the website unblocked:

E.g. students need to access it for classwork, homework, revision

Can we re-block this site after a specific date?

No ☐ Yes ☐

Date the website can be re-blocked: _____

Signed:..... (Safeguarding Lead)

This must be signed before website is unblocked.

.....

TECHNICIAN USE:

Date website unblocked:

If the website is not unblocked please explain why: