NORTHWEST
LONDON JEWISH DAY SCHOOL
Striving to achieve excellence for all

E-Safety Policy

Contents

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
- COVID 19 Addendum
- Data Protection Policy
- Behaviour Policy
- Anti-bullying Policy

Safeguarding team and Key Staff members:

Safeguarding Lead	Miss Judith Caplan (Headteacher)
Deputy Safeguarding Leads	Rabbi Ronen Broder Mr Yosh Radomsky
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	Mr Ashley Donoff
Safeguarding Trustee	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 North West London 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 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.

Dangers to Consider

Some of the dangers children may face include

- Access to illegal, harmful or inappropriate images or other content
- 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.

Mobile phones

Mobile phones must be on silent whilst in the building. Staff are permitted to take photos on their mobile phones, for educational purpose, provided that it is uploaded to the school server and then deleted from their phones that same day. SLT have the right to request proof of this

Children are not permitted to have mobile phones on site. Those who walk to and from school and therefore for safety have a phone they should hand these into the school as they arrive and collect at the end of the day.

ICT-BASED FORMS OF ABUSE

(This section of the policy was specifically prepared with reference to DfE guidance and is also an appendix to the Anti-Bullying Policy.)

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.

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 cyber-bullying. 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.

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 /Safeguarding Lead	National online safety certified Level 3 certificate in online Safety for DSLs	Annually
Deputy safeguarding lead	National online safety certified Level 3 certificate in online Safety for DSLs	Annually
Child Protection Teacher	National online safety certified Level 3 certificate in online Safety for DSLs	Annually
Staff	1. Updates at the start of each term. 2. National online safety CPD	Termly and more frequently if needed. Annually
Governors/Trustees	1. Updated annually at a	Annually and more frequently if needed.

	governors meeting 2. National online safety CPD	
Parents	Online safety course either via The National online CPD site or via Child Protect Education	Annually And when required throughout the year
Children	Each class has at least 3 sessions each academic year (see below) All IT sessions have an E-Safety element to it. Year 6 receive online safety workshop linked with secondary transfer	Termly and more frequently should anything arise.

Pupils have at least 3 training sessions during an academic year. One takes place each term. Usually two sessions are run by trained external providers and one is lead as part of a PSHE session. 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**
- https://www.thinkuknow.co.uk/parents/Listing/?cat=75&ref=4824&keyWord= - **think you know website link to films**
- **These are more for EYFS and KS1**
- http://hectorsworld.netsafe.org.nz/teachers/lesson-plans-and-resources/ - Hectors world resources and lesson plans
- https://www.youtube.com/watch?v=uRkpf0bk3P4 – video Hectors world – 1 (
- https://www.youtube.com/watch?v=XUAXS3P9sDE – hectors World video 2
- https://www.youtube.com/watch?v=6cibv8dx5JM – hectors world - Keeping your personal information safe - Episode 3

Reporting

We take all concerns seriously. All online concerns are reported to the E-Safety lead and followed up. Where there are Child Protection concerns the Child Protection team are informed. Parents are also informed of a concern so that we work in collaboration to keep children safe.

Children and online safety away from school

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.

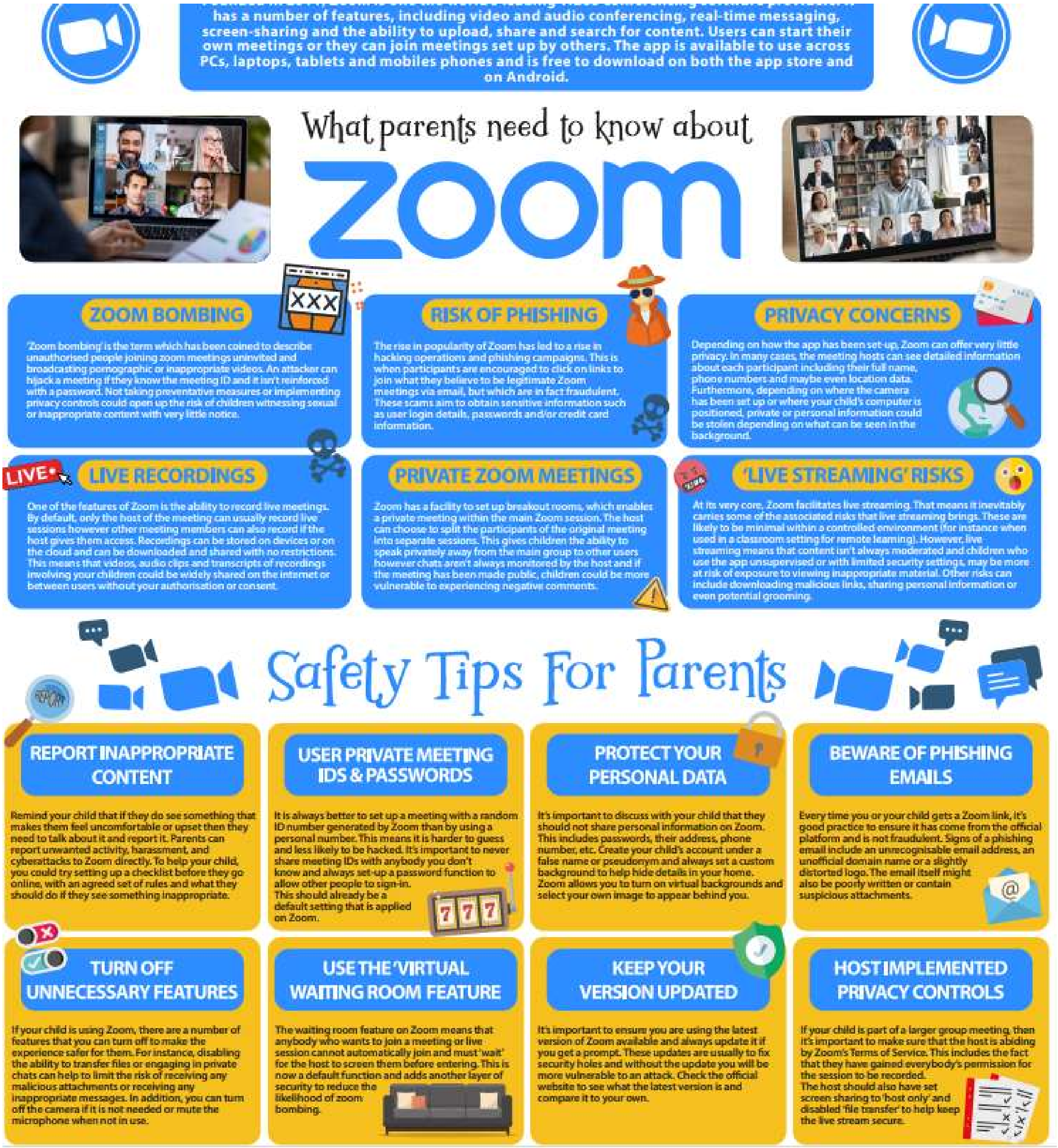
North West London Jewish Day School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- best practice is to hold group sessions of session with more than one pupils in, if there is a one to one session for an SEN child then their parent should be present.
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms provided by North West London Jewish Day School to communicate with pupils
- Staff should record, the length, time, date and attendance of any sessions held.

The school use Zoom as part of their online platform for meetings internally, externally and for sessions. Staff are reminded each week about online safety requirements in staff meetings. Parents are also sent information about keeping children safe whilst using zoom (see appendix 1)

Appendix 1



has a number of features, including video and audio conferencing, real-time messaging, screen-sharing and the ability to upload, share and search for content. Users can start their own meetings or they can join meetings set up by others. The app is available to use across PCs, laptops, tablets and mobiles phones and is free to download on both the app store and on Android.

What parents need to know about ZOOM

ZOOM BOMBING

'Zoom bombing' is the term which has been coined to describe unauthorised people joining zoom meetings uninvited and broadcasting pornographic or inappropriate videos. An attacker can hijack a meeting if they know the meeting ID and it isn't reinforced with a password. Not taking preventative measures or implementing privacy controls could open up the risk of children witnessing sexual or inappropriate content with very little notice.

RISK OF PHISHING

The rise in popularity of Zoom has led to a rise in hacking operations and phishing campaigns. This is when participants are encouraged to click on links to join what they believe to be legitimate Zoom meetings via email, but which are in fact fraudulent. These scams aim to obtain sensitive information such as user login details, passwords and/or credit card information.

PRIVACY CONCERNS

Depending on how the app has been set-up, Zoom can offer very little privacy. In many cases, the meeting hosts can see detailed information about each participant including their full name, phone numbers and maybe even location data. Furthermore, depending on where the camera has been set up or where your child's computer is positioned, private or personal information could be stolen depending on what can be seen in the background.

LIVE RECORDINGS

One of the features of Zoom is the ability to record live meetings. By default, only the host of the meeting can usually record live sessions however other meeting members can also record if the host gives them access. Recordings can be stored on devices or on the cloud and can be downloaded and shared with no restrictions. This means that videos, audio clips and transcripts of recordings involving your children could be widely shared on the internet or between users without your authorisation or consent.

PRIVATE ZOOM MEETINGS

Zoom has a facility to set up breakout rooms, which enables a private meeting within the main Zoom session. The host can choose to split the participants of the original meeting into separate sessions. This gives children the ability to speak privately away from the main group to other users however chats aren't always monitored by the host and if the meeting has been made public, children could be more vulnerable to experiencing negative comments.

'LIVE STREAMING' RISKS

At its very core, Zoom facilitates live-streaming. That means it inevitably carries some of the associated risks that live streaming brings. These are likely to be minimal within a controlled environment (for instance when used in a classroom setting for remote learning). However, live streaming means that content isn't always moderated and children who use the app unsupervised or with limited security settings, may be more at risk of exposure to viewing inappropriate material. Other risks can include downloading malicious links, sharing personal information or even potential grooming.

Safety Tips For Parents

REPORT INAPPROPRIATE CONTENT

Remind your child that if they do see something that makes them feel uncomfortable or upset then they need to talk about it and report it. Parents can report unwanted activity, harassment, and cyberattacks to Zoom directly. To help your child, you could try setting up a checklist before they go online, with an agreed set of rules and what they should do if they see something inappropriate.

USER PRIVATE MEETING IDS & PASSWORDS

It is always better to set up a meeting with a random ID number generated by Zoom than by using a personal number. This means it is harder to guess and less likely to be hacked. It's important to never share meeting IDs with anybody you don't know and always set-up a password function to allow other people to sign-in.
This should already be a default setting that is applied on Zoom.

PROTECT YOUR PERSONAL DATA

It's important to discuss with your child that they should not share personal information on Zoom. This includes passwords, their address, phone number, etc. Create your child's account under a false name or pseudonym and always set a custom background to help hide details in your home. Zoom allows you to turn on virtual backgrounds and select your own image to appear behind you.

BEWARE OF PHISHING EMAILS

Every time you or your child gets a Zoom link, it's good practice to ensure it has come from the official platform and is not fraudulent. Signs of a phishing email include an unrecognisable email address, an unofficial domain name or a slightly distorted logo. The email itself might also be poorly written or contain suspicious attachments.

TURN OFF UNNECESSARY FEATURES

If your child is using Zoom, there are a number of features that you can turn off to make the experience safer for them. For instance, disabling the ability to transfer files or engaging in private chats can help to limit the risk of receiving any malicious attachments or receiving any inappropriate messages. In addition, you can turn off the camera if it is not needed or mute the microphone when not in use.

USE THE 'VIRTUAL WAITING ROOM FEATURE

The waiting room feature on Zoom means that anybody who wants to join a meeting or live session cannot automatically join and must 'wait' for the host to screen them before entering. This is now a default function and adds another layer of security to reduce the likelihood of zoom bombing.

KEEP YOUR VERSION UPDATED

It's important to ensure you are using the latest version of Zoom available and always update it if you get a prompt. These updates are usually to fix security holes and without the update you will be more vulnerable to an attack. Check the official website to see what the latest version is and compare it to your own.

HOST IMPLEMENTED PRIVACY CONTROLS

If your child is part of a larger group meeting, then it's important to make sure that the host is abiding by Zoom's Terms of Service. This includes the fact that they have gained everybody's permission for the session to be recorded.
The host should also have set screen sharing to 'host only' and disabled 'file transfer' to help keep the live stream secure.