



NORTH WEST LONDON JEWISH DAY SCHOOL

E-SAFETY

POLICY

First Written: October 2012 Updated: April 2014



CONTENTS PAGE

Rationale	page 2
Development	page 3
Review of this Policy	page 3
Monitoring	page 3
Scope of the Policy	page 3
Roles and Responsibilities	
Governors	page 4
Head teacher and Senior Management	page 4
ICT Coordinator	page 4
Technical Staff	page 5
Teaching and support staff	page 5
Designated person for Child Protection	page 5
Pupils	page 6
Parents	page 6
E Safety in the classroom	page 6
Technical- infrastructure	page 7
Data Protection	page 7
Acceptable use policies	page 8
Legislation	page 10
Links to E-Safety and Data Handling websites	page 13



Rationale

North West London Jewish Day School has put this E-safety policy in place to ensure the safeguarding of its whole school community; staff, parents/carers, children and Governors. This policy states how we intend to do this in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

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

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



Development

North West London Jewish Day School's Policy is written by the Designated E-Safety teacher together with the ICT Coordinator, Headteacher and teacher incharge of Safeguarging and Child Protection.

All staff and Governors will be given a copy to look at and comment on. Comments from all stakeholders will be considered and discussed, amendments will be made and the policy will be presented to the whole governing body and Trustees. Once the Governors have approved the contents of the policy, then the wider community will be informed of its content and asked to sign the acceptable use policies.

Review of this Policy

The E –Safety Policy will be reviewed every Year and earlier should a new piece of legislation come into power or an issue arises. The policy will also be in line with the statutory requirements of the National Curriculum. Should any amendments be made all people whom may be affected by the amendments will be informed.

Monitoring

There will also be a log book for any reported incidences, this will be kept with the Technician, who will look at this book as part of his weekly responsibilities and report to the; designated E-Safety Teacher, ICT Coordinator(s), Child Protection Teacher and Head teacher.

ScopeofthePolicy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.



Rolesand Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors who are responsible for ICT and Safeguarding, receiving regular information about e-safety incidents and monitoring reports.

The role of the E-Safety Governor will include:

- Ensuring all governors attend e-safety training each year.
- regularly updating governors with issues relating to e-safety
- keeping up to date with the changes to e-safety.

Headteacher and Senior Management Team:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ICT Coordinator.
- The Headteacher and Management team are responsible for ensuring that the person in charge of E-Safety, the technician and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues.
- The Headteacher will ensure that the person in charge of Child Protection within the school is inform of any issue that may arise involving E-Safety.
- The Head teacher and Management team will receive regular updates from the person in charge of E-Safety and log book, and will act upon any action that may need to be taken..
- The Headteacher and Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

ICT Coordinator/Teacher in charge of ICT/Person in charge of E-Safety:

The responsibilities of the person in charge of E-Safety are:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies
- 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 training and advice for staff
- Go on any CPD courses and report back to staff.
- liaises with school ICT technician and monitors the log book
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meet termly with the headteacher, ICT Governor and Technician discuss current issues, review incident logs and filtering
- Ensure that all staff including office staff, parents/carers and pupils have read, and signed the acceptable use policy.
- Monitor that visitors to the school sign the correct acceptable use policy: this is to include; Sports coaches, parent helpers who do not have children in the school (ie grandparents,), security, caretakers and any outside agency that needs to use any technical equipment. This technical equipment can be the schools or their own.



Technical staff:

The ICT Technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the ICT Coordinator or person in charge of E-Safety.
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their esafety role and to inform and update others as relevant
- that the log book is accessible to all staff members
- that any incidences are reported immediately to the ICT Coordinator or person in charge of E-Safety and the Head teacher.
- that he/she attends regular termly meeting with the Head teacher, ICT Governor, ICT coordinator and person in charge of E-Safety

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- that at the start of each academic year they talk about safety and show the children the think u know website
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned teachers ensure that they have checked the sights to be suitable for their use
- any E-Safety issue that arises should be written in the E-Safety log book in the technicians office AND reported to the E-Safety officer.

Designated person for child protection

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying



Students/pupils:

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, curriculum evening, newsletters, letters, website and VLE

Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website and the school VLE in accordance with the relevant school Acceptable Use Policy.
- Attend E-Safety training each year through PTA event or curriculum evening

E-SAFTEY IN THE CLASSROOM

Education-students/pupils

The education of all pupils in e-safety is an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways: (

- A planned e-safety programme should be provided as part of ICT and PHSE /SEAL and delivered by both the class teacher and the person responsible for E-Safety.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies
- pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Rules for use of ICT systems will be posted in the ICT suite and on the MLE as children log in.
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- staff will have E-Safety training each academic year.
- The E-Safety coordinator is responsible for ensuring all new staff are trained and aware of the E Safety in place at North West London Jewish Day School.



Technical-infrastructure / equipment, filtering and monitoring

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

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to the Headteacher.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However there are risks to this and at North west London Jewish Day School All staff should be aware that any digital recording that is carried out should NOT be done without written consent from parent/carers and should NOT be posted on the internet.

These digital images are to be kept saved on an encrypted USB. They maybe posted on the schools MLE. But may not be posted by any other school.

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:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school 's Data Security checklist is checked regularly by the teacher in charge of ICT and the school Technician.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on encrypted USBs, secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.



Responding to incidents of misuse

These will be recorded in the school E Safety book located by the Technicians office. They will also be reported to the Child protection officer, teacher in charge of ESafety and the Headteacher.

If any apparent or actual misuse appears to involve illegal activity such as ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Then the head teacher will be informed and he/she will be responsible for informing the Local authority, Governors and in some cases the police.

If these involve the Child Protection Teacher then the headteacher will be informed in the first instants. If this involves the head teacher then this should be reported in the first instants to the Local Authority and they will give clear instructions who to contact next.

Acceptable use policies

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

There are 3 Acceptable Use Policies. One for children in Key Stage 1, One for Children in Key Stage 2 and one for teaching and non teaching staff – this one includes visitors and Governors.

All visitors who use any digital technology must sign a copy of the acceptable use policy on entry to the school.

Parents are asked to sign an acceptable use policy at the start of each academic year this also includes permission for photos of their child to be taken.



The following members of staff are involved with the provision of E-Safety at North West London Jewish Day School.

POSITION	DESIGNATED MEMBER OF STAFF OR GOVENOR
HEADTEACHER	Rabbi Daniel Kerbel
TEACHER INCHARGE OF CHILD PROTECTION	Mrs Madeleine Bendel
TEACHER INCHARGE OF E-SAFETY	Miss Judith Caplan
CHAIR OF GOVENORS	Mr Paul Gotlieb
E-SAFETY AND SAFEGUARDING GOVENOR	Mrs Sheila Taylor
ICT GOVENOR	Mr Herman Martyn/ Mrs Arielle Scemama
TEACHER IN CHARGE OF ICT	Miss Camilla Kahn
TECHNICIAN	Mr Sylvester Saldanha

MOBILE PHONE:

The use of mobile phones is not permitted by the children. It is a breach of a child's human rights to take a child's mobile phone if this is not in the behaviour policy (See behaviour policy). Children who travel to and from school independently and therefore have a mobile phone should hand the phone into the school office on their arrival and collect it at the end of the school day.

Any child who is found with a mobile phone will be asked to hand it to the school office and their parent/carer will have to collect it at the end of the school day. Letters are sent to the the upper key stage 2 parents at the start of each academic year informing them of this. This is also mentioned to parents in Years 5 and 6 at the Curriculum Meeting at the start of the academic year.

Staff are permitted to have mobile phones but are advised not to take pictures of children with it.



Legislation

Schools should be aware of the legislative framework under which this E-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.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

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.

Data Protection Act 1998

This protects the rights and privacy of 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.

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 help line staff.
- The school 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 Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks 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 Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows 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 him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so 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 a 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

The new 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 Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.



Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-safety policy.

SOUTH WEST GRID FOR LEARNING:

"SWGfL Safe" - http://www.swgfl.org.uk/safety/default.asp

Child Exploitation and Online Protection Centre (CEOP)

http://www.ceop.gov.uk/

ThinkUKnow http://www.thinkuknow.co.uk/

CHILDNET http://www.childnet-int.org/

INSAFE http://www.saferinternet.org/ww/en/pub/insafe/index.htm

BYRON REVIEW ("Safer Children in a Digital World") http://www.dcsf.gov.uk/byronreview/

Becta

Website e-safety section - http://schools.becta.org.uk/index.php?section=is

Developing whole school policies to support effective practice:

http://publications.becta.org.uk/display.cfm?resID=25934&page=1835

Signposts to safety: Teaching e-safety at Key Stages 1 and 2 and at Key Stages 3 and 4:

http://publications.becta.org.uk/display.cfm?resID=32422&page=1835

"Safeguarding Children in a Digital World"

http://schools.becta.org.uk/index.php?section=is&catcode=ss to es tl rs 03&rid=13344

LONDON GRID FOR LEARNING

http://cms.lgfl.net/web/lgfl/365

KENT NGfL

http://www.kented.org.uk/ngfl/ict/safety.htm

NORTHERN GRID

http://www.northerngrid.org/ngflwebsite/esafety_server/home.asp

NATIONAL EDUCATION NETWORK

NEN E-Safety Audit Tool: http://www.nen.gov.uk/hot topic/13/nen-e-safety-audit-tool.html

CYBER-BULLYING

DCSF - Cyberbullying guidance <u>http://publications.teachernet.gov.uk/default.aspx?PageFunction=productdetails&PageMode=spectrum&P</u> <u>roductId=DCSF-00658-2007</u>

Teachernet

http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullving/cyberbullving/

Teachernet "Safe to Learn – embedding anti-bullying work in schools" http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/

Anti-Bullying Network - http://www.antibullying.net/cvberbullying1.htm

Cyberbullying.org - <u>http://www.cyberbullying.org/</u>



East Sussex Council – Cyberbullying - A Guide for Schools: https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullving/Pages/eastsussexandnationalg uidance.aspx

References to other relevant anti-bullying organisations can be found in the appendix to the DCSF publication "Safe to Learn" (see above)

SOCIAL NETWORKING

Home Office Task Force - Social Networking Guidance http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce

Digizen - "Young People and Social Networking Services": http://www.digizen.org.uk/socialnetworking/

Ofcom Report:

http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/

MOBILE TECHNOLOGIES

"How mobile phones help learning in secondary schools": http://partners.becta.org.uk/index.php?section=rh&catcode= re rp 02 a&rid=15482

Mobile phones and cameras:

http://schools.becta.org.uk/index.php?section=is&catcode=ss to es pp mob 03

DATA PROTECTION AND INFORMATION HANDLING

Information Commissioners Office - Data Protection: http://www.ico.gov.uk/Home/what we cover/data protection.aspx

BECTA - Data Protection: http://schools.becta.org.uk/index.php?section=lv&catcode=ss lv saf dp 03

PARENTS GUIDES TO NEW TECHNOLOGIES AND SOCIAL NETWORKING: http://www.iab.ie/

Policy review date:

.....