Rimon
Jewish Primary School

E-Safety Policy

This e-safety policy is consistent with related school policies such as Safeguarding, Anti-Bullying, Behaviour, the Email and Acceptable Use of the Internet Policy and the Email and Internet User Agreement.

Introduction

Children are "digital natives" growing up in a world dominated by information and communications technology that provides them with access to a wide range of information and increased opportunities for instant communication and social networking. Using the internet can benefit children's education and give them more opportunities to socialise, but it can also present several risks. Children are often unaware that they are as much at risk online as they are in the real world.

It is Rimon's policy that the educational and social benefits of the internet should be promoted, but that this should be balanced against the need to safeguard children. To achieve this, the school has an e-safety strategy working in partnership with parents to recognise the risks and take action to help children use the internet safely and responsibly.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.facebook.com www.myspace.com www.piczo.com www.bebo.com)
- Video broadcasting sites (Popular: http://www.youtube.com)
- Chat Rooms (Popular www.teenchat.com www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com http://www.miniclip.com/games/en/ http://www.runescape.com, http://www.clubpenguin.com)
- Music download sites (Popular http://www.apple.com/ituneshttp www.napster.co.uk http://www-kazzaa.com)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications

Benefits of ICT

Use of ICT is so universal that it is of huge benefit to children to learn these skills in order to prepare themselves for the working environment. The internet can make a huge contribution to children's education and social development by:

- raising educational attainment, engaging and motivating pupils to learn and improving their confidence
- improving pupil's research and writing skills
- allowing children with disabilities to overcome communications barriers
- enabling children to be taught "remotely", for example children who are unable to attend school
- improving pupil's wellbeing through the social and communications opportunities offered
- providing access to a wide range of educational materials and teaching resources.

Risks

The risk associated with use of ICT by children can be grouped into 4 categories: content, contact, culture and commerce.

Content

The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. There is a danger that children may be exposed to inappropriate images such as pornography, or information advocating violence, racism or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

Contact

Chat rooms and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent. The internet may also be used as a way of bullying a child, known as cyber bullying.

Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Disclosing this information can lead to fraud or identity theft.

Culture

Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

- becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
- using information from the internet in a way that breaches copyright laws
- uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience
- cyber bullying (also see Anti-Bullying Policy).

Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment.

Definition and purpose of E-Safety
E-safety forms part of the school's safeguarding procedures and anti-bullying measures. All schools have a responsibility under the Children Act 2004 to safeguard and promote the welfare of pupils, as well as owing a duty of care to children and their parents to provide a safe learning environment.

E-safety is a framework of policy, practice, education and technological support that ensures a safe e-learning environment in order to maximise the educational benefits of ICT whilst minimising the associated risks.

This e-safety policy and strategy enables Rimon to create a safe e-learning environment that:

- promotes the teaching of ICT within the curriculum
- protects children from harm
- safeguards staff in their contact with pupils and their own use of the internet
- ensures the school fulfils its duty of care to pupils
- provides clear expectations for staff and pupils on acceptable use of the internet.

Elements of E-Safety
Rimon enables an "e-safe" environment for pupils by ensuring that the following aspects are addressed:

Safe Systems
Rimon ensures that the Internet provided offers a safe e-learning environment by providing filtering software to block access to unsuitable sites, anti-virus software and Internet monitoring systems.

Safe Practices
Every parent, pupil and staff member signs Email and Internet User Agreement and the school has an Email and Use of the Internet Policy. It is the responsibility of all staff to be aware of the issues and know what is expected of them in terms of their own acceptable use of the internet and other technologies.

Safety Awareness
It is vital that children are able to keep themselves and others safe and use the internet responsibly. Working in partnership with parents and carers, Rimon takes

its role in raising pupils' awareness of the potential dangers of using the internet seriously and uses strategies to reduce this risk (CEOP training for staff and pupils and regular information about e-safety for parents.)

Roles and Responsibilities

Headteacher's role:

The Headteacher has ultimate responsibility for e-safety issues within the school including:

- the overall development and implementation of the school's e-safety policy
- ensuring that e-safety issues are given a high profile within the school community
- linking with the board of governors and parents and carers to promote e-safety and forward the school's e-safety strategy
- ensuring e-safety is embedded in the curriculum
- deciding on sanctions against staff and pupils who are in breach of acceptable use policies.

Governors' Roles:

The Governing body have a statutory responsibility for pupil safety, it is vital that governors are aware of e-safety issues and support the headteacher in the development of the school's e-safety policy and strategy and promote e-safety to parents.

E-Safety Officer's Role:

Rimon has a designated E-Safety Officer who is responsible for co-ordinating e-safety policies on behalf of the school. This is Dr Zoe Dunn who is also the designated child protection officer. The e-safety officer ensures they keep up to date with e-safety issues and guidance through liaison with the Local Authority E-Safety Officer and through organisations such as The Child Exploitation and Online Protection (CEOP). The e-safety contact officer has the authority, knowledge and experience to carry out the following:

- develop, implement, monitor and review the school's e-safety policy
- ensure that staff and pupils are aware that any e-safety incident should be reported to them
- provide the first point of contact and advice for school staff, governors, pupils and parents
- liaise with the school's IT manager to ensure they are kept up to date with e-safety issues and to advise of any new trends, incidents and arising problems to the head teacher
- assess the impact and risk of emerging technology and the school's response to this in association with IT staff and the Schools IT team
- raise the profile of e-safety awareness with the school by ensuring access to training and relevant e-safety literature
- ensure that all staff and pupils have read and signed the acceptable use policy
- report annually to the Governors on the implementation of the school's e-safety strategy

- maintain a log of internet related incidents and co-ordinate any investigation into breaches
- report all incidents and issues to Barnet's e-safety officer
- support any subsequent investigation into breaches and preserving any evidence.

The school's Internet provider and MIS system provider ensures the regular maintenance and monitoring of the school intranet, including anti-virus and filtering systems and helps to carry out monitoring and audits of networks and reporting breaches to the e-safety contact officer.

Role of School Staff:
Teaching staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is:

- adhering to the school's e-safety and acceptable use policy and procedures
- communicating the school's e-safety and acceptable use policy to pupils
- keeping pupils safe and ensuring they receive appropriate supervision and support whilst using the intranet
- planning use of the internet for lessons and researching on-line materials and resources
- reporting breaches of internet use to the e-safety contact officer
- recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the e-safety contact officer.

Designated Child Protection Officer:
Where any e-safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated child protection officer who will decide whether or not a referral should be made to Safeguarding and Social Care or the Police. The designated child protection teacher will be the e-safety contact officer: Dr Zoe Dunn.

Pupils with Special Needs
Pupils with learning difficulties or disability may be more vulnerable to risk from use of the internet and will require additional guidance on e-safety practice as well as closer supervision.

The SENCO is responsible for providing extra support for these pupils and should:

- link with the e-safety contact officer to discuss and agree whether the mainstream safeguarding systems on the intranet are adequate for pupils with special need.

- where necessary, liaise with the e-safety contact officer and the Schools IT team to discuss any requirements for further safeguards to the school intranet or tailored resources and materials in order to meet the needs of pupils with special needs

- ensure that the school's e-safety policy is adapted to suit the needs of pupils with special needs.

- liaise with parents, carers and other relevant agencies in developing e-safety practices for pupils with special needs

- keep up to date with any developments regarding emerging technologies and e-safety and how these may impact on pupils with special needs.

Working with Parents

Rimon sees parental involvement as integral to the success of its e-safety strategies as almost all children will have internet access at home and on mobile devices and might not be as closely supervised in its use as they would be at school.

- Parents will be provided with information on ICT learning and the school's e-safety policy

- Parents will be asked to sign acceptable use agreements on behalf of their child so that they are fully aware of their child's level of internet use within the school as well as the school's expectations regarding their behaviour.

- The Headteacher will give regular parent presentations on e-safety and will ensure that parents are frequently informed about how to keep their children safe online at home and when using mobile devices.

- Information about e-safety will be readily available to all parents to ensure that parents and carers are fully aware of e-safety issues so that they can extend e-safety strategies to the home environment.

Accessing and Monitoring the System

- Access to the intranet in primary schools should be via a class log-in and password; staff access should be via individual log-ins and passwords.

- The e-safety contact officer should keep a record of all log-ins used within the school for the purposes of monitoring and auditing internet activity.

- Network and technical staff responsible for monitoring systems should be supervised by a senior member of their management team.

- The e-safety contact officer and teaching staff should carefully consider the location of computer terminals in classrooms and teaching areas in order to allow an appropriate level of supervision of pupils depending on their age and experience.

Acceptable Use Policies

- All users of the intranet within the school will be expected to sign *the* Email and Internet User Agreement that sets out their rights and responsibilities and incorporates the school e-safety rules regarding their internet use.

- Acceptable use agreements will be signed by parents on their child's behalf at the same time that they give consent for their child to have access to the intranet in school (see appendix).

- Staff are expected to sign the *Email and Acceptable Use of the Internet Policy and* on appointment and this will be integrated into their general terms of employment (see the *Email and Acceptable Use of the Internet Policy*).

The e-safety officer will keep a copy of all signed acceptable use agreements.

Teaching E-Safety

Responsibility

One of the key features of Rimon's e-safety strategy is teaching pupils to protect themselves and behave responsibly while on-line. There is an expectation that over time, pupils will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

Overall responsibility for the design and co-ordination of e-safety education lies with the headteacher and the e-safety contact officer, but all teaching staff should play a role in delivering e-safety messages. The e-safety contact officer is responsible for ensuring that all staff have the knowledge and resources to enable them to do so.

Content

Pupils should be taught:

- the benefits and risks of using the internet
- how their behaviour can put themselves and others at risk
- what strategies they can use to keep themselves safe
- what to do if they are concerned about something they have seen or received via the internet
- who to contact to report concerns
- that the school has a "no blame" policy so that pupils are encouraged to report any e-safety incidents
- that the school has a "no tolerance" policy regarding cyber bullying
- the basic principles of "netiquette"
- behaviour that breaches acceptable use policies will be subject to sanctions and disciplinary action
- The internet should only be used for educational purposes
- The intranet has been designed so that use is monitored and that access to some sites are blocked
- the school's policy on using their own mobile phones whilst in school.

Delivering E-Safety Messages

Discussion: Many pupils are very familiar with the culture of new technologies, they can be involved in reviewing the School's e-safety practices, possibly through a student council. Pupils' perceptions of the risks may not be mature; the e-safety rules

will need to be explained or discussed. E-safety will be taught in all year groups, covering age-appropriate issues. Useful e-safety programmes include:

- Barnet and LGfL e-safety and e-literacy Framework for EYFS-Y6 (www. safety.lgfl.net)
- Think U Know; currently available for secondary pupils. (www.thinkuknow.co.uk/)
- Grid Club www.gridclub.com
- The BBC's ChatGuide: www.bbc.co.uk/chatguide

In addition it is delivered through the ICT and PSHE curriculum as well as through discrete CEOP training for pupils.

- Teachers are primarily responsible for delivering an on-going e-safety education in the classroom as part of the curriculum.

- Rules regarding safe internet use are posted up in all classrooms and teaching areas where computers are used to deliver lessons.

- The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe.

- Teachers may wish to use PSHE lessons as a forum for discussion on e-safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst on-line.

- Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills.

ICT and Safe Teaching Practice

Rimon staff are aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils. The following points are to be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations:

- Photographic and video images of pupils should only be taken by staff in connection with educational purposes, for example school trips and in the EFYS classroom for observations and profile evidence.

- Staff should always use school equipment and only store images on the school computer system, with all other copies of the images erased.

- Staff should take care regarding the content of and access to their own social networking sites and ensure that pupils and parents cannot gain access to these.

- Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal.

- Staff should be particularly careful regarding any comments to do with the school or specific pupils that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.

- Staff should not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context.

- Where staff need to communicate with pupils regarding school work, this should be via the intranet and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.

- When making contact with parents or pupils by telephone, staff should only use school equipment. Pupil or parent numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to pupils.

- Staff should ensure that personal data relating to pupils is stored securely and encrypted if taken off the school premises.

- Where staff are using mobile equipment such as laptops provided by the school, they should ensure that the equipment is kept safe and secure at all times.

Safe use of ICT

Internet and Search Engines

- When using the internet, children should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate children are the ones who are most at risk.

- Primary school children should be supervised at all times when using the internet. Although supervision of secondary school pupils will be more flexible, teachers should remain vigilant at all times during lessons.

- Pupils should not be allowed to aimlessly "surf" the internet and all use should have a clearly defined educational purpose.

- Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.

- Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the e-safety contact officer, who will liaise with the Schools IT team for temporary access.

- Teachers should notify the e-safety contact officer once access is no longer needed to ensure the site is blocked.

Evaluating and Using Internet Content

As the information generated by internet searches could be vast, and much of it irrelevant to the subject being taught, teachers should teach pupils good research skills that help them to maximise the resource. They should also be taught how to critically evaluate the information retrieved by:

- questioning the validity of the source of the information; whether the author's view is objective and what authority they carry

- carrying out comparisons with alternative sources of information

- considering whether the information is current and whether the facts stated are correct.

In addition, pupils should be taught the importance of respecting copyright and correctly quoting sources and told that plagiarism (copying others work without giving due acknowledgement) is against the rules of the school and may lead to disciplinary action.

Emails

The school intranet hosts an email system that allow pupils to send emails to others within the school or to approved email addresses externally.

- Access to and use of personal email accounts is forbidden and may be blocked. This is to protect pupils from receiving unsolicited mail and preserve the safety of the system from hacking and viruses.

- Emails should only be sent via the school intranet to addresses within the school system or approved external address.

- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the e-safety contact officer who will liaise with the Schools IT team.

- Pupils should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence.

- All email communications should be polite; if a pupil receives an offensive or distressing email, they should be instructed not to reply and to notify the responsible teacher immediately.

- Pupils should be warned that any bullying or harassment via email will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.

- Users should be aware that as use of e-mail via the intranet is for the purposes of education or school business only, and all emails may be monitored.

- Access to email systems by primary school pupils should be via a class email address only. Secondary school pupils should be issued with an individual account using their log-in and password.

- All email messages sent by pupils in connection with school business must be checked and cleared by the responsible teacher.
- Apart from the head teacher, individual email addresses for staff or pupils should not be published on the school website.

- Pupils should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

Social Networking Sites, Newsgroups and Forums

Social networking sites such as Facebook, MySpace and Bebo allow users to publish information about themselves to be seen by anyone who has access to the site. These sites are not allowed to be used in school but it is likely that pupils will use these sites at home. Parents and pupils will be informed about the recommended age for use of these sites,, i.e. 13 for Facebook and the e-safety office will inform parents if pupils are using these sites at an inappropriate age. In addition:

- Access to unregulated public social networking sites, newsgroups or forums should be blocked.

- If there is a clear educational use for these sites for on-line publishing, they should only use approved sites such as those provided via the intranet.

- Any use of these sites will be strictly supervised by the responsible teacher.

- Pupils will be warned that any bullying or harassment via social networking sites will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.

In order to teach pupils to stay safe on social networking sites outside of school, they will be advised:

- not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended

- not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted

- how to set up security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them

- to behave responsibly whilst on-line and keep communications polite

not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

Chat Rooms and Instant Messaging

Chat rooms are internet sites where users can join in "conversations" on-line; instant messaging allows instant communications between two people on-line. In most cases, pupils will use these at home although the school does host these applications.

- Access to public or unregulated chat rooms will be blocked except for the site hosted by the school intranet, which is to be used for educational purposes only.

- Pupils will be warned that any bullying or harassment via chat rooms or instant messaging taking place within or out of school will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.

In order to teach pupils to stay safe whilst using chat rooms outside of school, they will be advised:

- not to give out personal details to anyone on-line that may help to identify or locate them or anyone else

- only use moderated chat rooms that require registration and are specifically for their age group

- not to arrange to meet anyone whom they have only met on-line

- to behave responsibly whilst on-line and keep communications polite

- not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

Video Conferencing

Video conferencing enables users to communicate face-to-face via the internet using web cameras.

- Video conferencing should only be carried out using approved software via the school intranet.

- Teachers should avoid using other webcam sites on the internet due to the risk of them containing links to adult material. In the event that teachers do use other webcam sites, this should be discussed and agreed in advance with the school IT provider.

- Pupil use of video conferencing should be for educational purposes and should be supervised as appropriate to their age. Pupils must ask permission from the responsible teacher before making or receiving a video conference call.

- Teachers should ensure that pupils are appropriately dressed during any photography or filming and equipment must not be used in changing rooms or toilets.

- Photographic or video devices may be used by teachers only in connection with educational activities including school trips.

- Photographs and videos may only be downloaded onto the school's computer system with the permission of the network manager and should never enable individual pupils' names or other identifying information to be disclosed.

School Website

- Content will not be uploaded onto the school website unless it has been authorised by the e-safety contact officer and the headteacher, who are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law..

- To ensure the privacy and security of staff and pupils, the contact details on the website should be the school address, email and telephone number. No contact details for staff or pupils should be contained on the website. This excludes direct school staff emails,

- Children's full names will not be published on the website.

- Links to any external websites should be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

Photographic and Video Images

- Where the school uses photographs and videos of pupils for publicity purposes, for example on the school website, images should be carefully selected so that individual pupils cannot be easily identified. It is recommended that group photographs are used.

- Where photographs or videos of children are used, written permission must be obtained first from their parents or carers, who should be informed of the purpose of the image and where it will appear.

- Children's names should never be published where their photograph or video is being used.

- Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images.

- Images should be securely stored only on the school's computer system and all other copies deleted.

- Stored images should not be labelled with the child's name and all images held of children should be deleted once the child has left the school.

Staff Mobile Phones
In the Foundation Stage classroom personal mobile phones will be kept in the staff area and not used in the classroom. All teachers will use the school mobile phone on school trips. Class cameras will be used to record pupil progress and images will be regularly checked.

The police will be involved if there is any criminal element to misuse of the internet, mobile phones or any other form of electronic media.

Pupils own Mobile Phone/handheld Systems
The majority of pupils are likely to have mobile phones or other equipment that allows them to access internet services, and these can pose a problem in that their use may distract pupils during lessons and may be used for cyber bullying. However, many parents prefer their children to have mobile phones with them in order to ensure their safety and enable them to contact home if they need to.

Rimon will allow pupils in Year 6 to have a mobile phone on the school premises, but pupils will need to hand these into the school office where they will be securely kept during the day and returned to pupils as they leave school. Parents will need to sign an agreement that enables their child to have a mobile phone in school.

Responding to Incidents

Policy Statement
All incidents and complaints relating to e-safety and unacceptable internet use will be reported to the e-safety contact officer in the first instance. All incidents, whether involving pupils or staff, must be recorded by the e-safety contact officer on the e-safety incident report form (see appendix).

A copy of the incident record should be sent to Barnet's designated e-safety officer.

Where the incident or complaint relates to a member of staff, the matter must always be referred to the headteacher for action. Incidents involving the headteacher should be reported to the Chair of Governors.

The school's e-safety officer should keep a log of all e-safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's e-safety system, and use these to update the e-safety policy.

E-safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the designated child protection teacher, who will make a decision as to whether or not to refer the matter to the police and/or Safeguarding and Social Care in conjunction with the head teacher.

Although it is intended that e-safety strategies and polices should reduce the risk to pupils whilst on-line, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. The school can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

Unintentional Access of Inappropriate Websites

- If a pupil or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen.

- Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the e-safety message and to demonstrate the school's "no blame" approach.

- The incident should be reported to the e-safety contact officer and details of the website address and URL provided.

- The e-safety officer should liaise with the network manager to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.

- It is essential that teachers ensure that where they have an asked for filtering to be lifted for a particular lesson (e.g.: sex education) that they notify the IT team so that filtering can be put back to minimise the risk of inappropriate sites being accessed by pupils or staff.

Intentional Access of Inappropriate Websites by Pupil

- If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions

- The incident should be reported to the e-safety officer and details of the website address and URL recorded.

- The e-safety contact officer should liaise with the network manager or Schools IT team to ensure that access to the site is blocked.

- The pupil's parents should be notified of the incident and what action will be taken.

Sanctions for Misuse of School ICT

Sanctions applied will reflect the seriousness of the breach and should take into account all other relevant factors.

Sanctions for Pupils

Category A Infringements

These are basically low-level breaches of acceptable use agreements such as:

- use of non-educational sites during lessons
- unauthorised use of email or mobile phones
- unauthorised use of prohibited sites for instant messaging or social networking.

Sanctions include referral to the class teacher or tutor as well as a referral to the e-safety contact officer.

Category B Infringements
These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of e-safety policy that are non-deliberate, such as:

- continued use of non-educational sites during lessons
- continued unauthorised use of email or mobile phones
- continued use of prohibited sites for instant messaging or social networking
- Sharing inappropriate emails with peers- low level cyber bullying
- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying staff
- accidentally accessing offensive material without notifying staff.

Sanctions include:

- referral to class teacher or tutor
- referral to e-safety contact officer
- loss of internet access for a period of time
- removal of mobile phone until the end of the day
- contacting parents.

Category C Infringements
These are deliberate actions that either negatively affect or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- deliberately bypassing security or access
- deliberately corrupting or destroying other people's data or violating other's privacy
- cyber bullying
- deliberately accessing, sending or distributing offensive or pornographic material
- purchasing or ordering items over the internet
- transmission of commercial or advertising material.

Sanctions could include:

- referral to class teacher or tutor
- referral to e-safety contact officer
- referral to head teacher
- loss of access to the internet and intranet for a period of time
- contact with parents
- any sanctions agreed under other school policies (Behaviour Policy)

Category D Infringements
These are continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal materials which may result in a criminal offence, such as:

- persistent and/or extreme cyber bullying
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Sanctions include:

- referral to head teacher
- contact with parents
- possible exclusion
- removal of equipment
- referral to community police officer
- referral to Camden's e-safety officer.

Inappropriate Use of ICT by Staff

- If a member of staff witnesses misuse of ICT by a colleague, they should report this to the head teacher and the e-safety officer immediately.

- The e-safety officer should notify the network manager so that the computer or laptop is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded on the e-safety incident report form.

- The e-safety officer should arrange with the network manager or Schools IT team to carry out an audit of use to establish which user is responsible and the details of materials accessed.

- Once the facts are established, the headteacher should take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate.

- If the materials viewed are illegal in nature the headteacher should report the incident to the police and follow their advice, which should also be recorded on the e-safety incident report form.

Sanctions for Staff

These should reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children.

Category A Infringements

These are minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the head teacher.

- excessive use of internet for personal activities not connected to professional development

- use of personal data storage media (eg: removable memory sticks) without carrying out virus checks
- any behaviour on the world wide web that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or pupils or inappropriate material published on social networking sites
- sharing or disclosing passwords to others or using other user's passwords
- breaching copyright or licence by installing unlicensed software.

Category B Infringements
These infringements involve deliberate actions that undermine safety on the internet and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or Safeguarding and Social Care.

- serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications
- any deliberate attempt to breach data protection or computer security rules, for example hacking
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Sanctions include:
- referral to the head teacher
- removal of equipment
- referral to Camden's e-safety officer
- referral to SSC or police
- suspension pending investigation
- disciplinary action in line with school policies

Cyber Bullying
Cyber bullying is defined as the use of ICT to deliberately hurt or upset someone. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience. Bullying may take the form of:

- rude, abusive or threatening messages via email or text
- posting insulting, derogatory or defamatory statements on blogs or social networking sites
- setting up websites that specifically target the victim
- making or sharing derogatory or embarrassing videos of someone via mobile phone or email (for example, "happy slapping").

Cyber bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases,

cyber bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

Dealing with Incidents
The following covers all incidents of bullying that involve pupils at the school, whether or not they take place on school premises or outside school.

- Rimon's anti-bullying and behaviour policies and the *Email and Acceptable Use of the Internet Policy and the* Email and Internet User Agreement policies cover the issue of cyber bullying and set out clear expectations of behaviour and sanctions for any breach.

- Any incidents of cyber bullying should be reported to the e-safety officer who will notify record the incident on the incident report form and ensure that the incident is dealt with in line with the school's anti-bullying policy. Incidents should be monitored and the information used to inform the development of anti-bullying policies.

- Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.

- As part of e-safety awareness and education, pupils should be told of the "no tolerance" policy for cyber bullying and encouraged to report any incidents to their teacher.

Pupils should be taught:

- to only give out mobile phone numbers and email addresses to people they trust
- to only allow close friends whom they trust to have access to their social networking page
- not to respond to offensive messages
- to report the matter to their parents and teacher immediately.
- Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.

Cyber Bullying of Teachers
Headteachers should be aware that teachers may become victims of cyber bullying by pupils. Because of the duty of care owed to staff, headteachers should ensure that teachers are able to report incidents in confidence and receive adequate support, including taking any appropriate action against pupils.

Incidents of cyber bullying involving teachers should be recorded and monitored by the e-safety contact officer in the same manner as incidents involving pupils. Teachers should follow the advice above on cyber bullying of pupils and not reply to messages but report the incident to the head teacher immediately.

Risk from Inappropriate Contacts

Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met on-line.

- All concerns around inappropriate contacts should be reported to the e-safety contact officer and the designated child protection teacher.

- The designated child protection teacher should discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to Safeguarding and Social Care and/or the police.

- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.

- The designated child protection teacher can seek advice on possible courses of action from Barnet's e-safety officer in Safeguarding and Social Care.

- Teachers should advise the pupil how to terminate the contact and change contact details where necessary to ensure no further contact.

- The designated child protection teacher and the e-safety contact officer should always notify the pupil's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.

- Where inappropriate contacts have taken place using school ICT equipment or networks, the e-safety contact officer should make a note of all actions taken and contact the network manager or Schools IT team to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.

This policy is part of our safeguarding group of policies: Allegations of Abuse made Against a member of Staff, Child Protection, Safer Recruitment, Behaviour, Health and Safety and Frist Aid.

June 2012
Reviewed at the discretion of the Governors

Rules For Online Safety

We only use the internet when an adult is with us.

We only click on the buttons or links when we know what they do.

We search the Internet with an adult, and we only use sites for schoolwork and homework.

We always ask if we get lost on the Internet.

We send and open emails together.

We only write polite and friendly emails to people that we know

I will not give my name, address or telephone number to anyone on the Internet and I will tell an adult if anyone asks me for my name, address or telephone number.

I will NEVER agree to meet someone I have spoken to on the Internet.

I will not download programmes or bring programmes from home into school.

Rimon Jewish Primary School

E-safety Incident Report Form

This form should be kept on file and a copy emailed to Barnet's e-safety officer.

School/organisation's details:

Name of school/organisation:

Address:

Name of e-safety contact officer:

Contact details:

Details of incident

Date happened:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?
□ In school/service setting □ Outside school/service setting

Who was involved in the incident?
□ child/young person □ staff member □ other (please specify

Type of incident:
□ bullying or harassment (cyber bullying
□ deliberately bypassing security or access
□ hacking or virus propagation
□ racist, sexist, homophobic religious hate material
□ terrorist material
□ drug/bomb making material
□ child abuse images
□ on-line gambling
□ soft core pornographic material
□ illegal hard core pornographic material
□ other (please specify)

Description of incident

Nature of incident

□ **Deliberate access**

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Could the incident be considered as;
□ harassment □ grooming □ cyber bullying □ breach of AUP

□ **Accidental access**

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Action taken

Staff

□ incident reported to head teacher/senior manager
□ advice sought from Safeguarding and Social Care
□ referral made to Safeguarding and Social Care
□ incident reported to police
□ incident reported to Internet Watch Foundation
□ incident reported to IT
□ disciplinary action to be taken
□ e-safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment)

Child/young person

□ incident reported to head teacher/senior manager
□ advice sought from Safeguarding and Social Care
□ referral made to Safeguarding and Social Care
□ incident reported to police
□ incident reported to social networking site
□ incident reported to IT
□ child's parents informed
□ disciplinary action to be taken
□ child/young person debriefed
□ e-safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment)

Outcome of incident/investigation