Shalom Noam Primary School

Online Safety Policy

September 2020

Online-Safety		
Date	**Review Date**	**Coordinator**
19/9/2020	**19/9/2021**	**Rabbi Cohen**

We believe this policy relates to the following legislation:

- Obscene Publications Act 1959
- Children Act 1989
- Computer Misuse Act 1990
- Education Act 1996
- Education Act 1997
- Police Act 1997
- Data Protection Act 1998
- Human Rights Act 1998
- Standards and Framework Act 1998
- Freedom of Information Act 2000
- Education Act 2003
- Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Children and Young Persons Act 2008
- School Staffing (England) Regulations 2009
- Equality Act 2010
- Education Act 2011
- Protection of Freedoms Act 2012

The following documentation is also related to this policy:

- Dealing with Allegations of Abuse against Teachers and other Staff: Guidance for Local Authorities, Headteachers, School Staff, Governing Bodies and Proprietors of Independent Schools (DfE)
- Equality Act 2010: Advice for Schools (DfE)
- Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges (DfE)
- Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children

We believe we have a duty to provide pupils with quality Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills as it is an essential element in 21st Century life for education and business life.

We believe that used correctly Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the school's management information and business administration systems

We acknowledge that the increased provision of the Internet in and out of school brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate Internet information and to take care of their own safety and security.

Online-Safety, which encompasses Internet technologies and electronic communications, will educate pupils about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.

We believe all pupils and other members of the school community have an entitlement to safe Internet access at all times.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that is connected with this policy.

Aims

- To provide pupils with quality Internet access as part of their learning experience across all curricular areas.
- To provide clear advice and guidance in order to ensure that all Internet users are aware of the risks and the benefits of using the Internet.
- To evaluate Internet information and to take care of their own safety and security.
- To raise educational standards and promote pupil achievement.

Responsibility of the Policy and Procedure

Role of the Governing Body

The Governing Body has:

- appointed a member of staff to be responsible for online-Safety;
- delegated powers and responsibilities to the Headteacher to ensure all school staff and stakeholders are aware of and comply with this policy;

Role of the Headteacher

The Headteacher will:

- ensure the safety and online-Safety of all members of the school community;
- ensure a safe and secure username / password system is in place for all:

  - technical systems;
  - networks;
  - devices; and
  - email and Virtual Learning Environments.
  - ensure all users are responsible for:

- the security of their username and password;
- not allowing other users to use this information to access the system;
- reporting any suspicion or evidence that there has been a breach of security;
- changing their password at regular intervals
- be responsible for the day to day online-Safety issues;
- ensure all school staff, pupils and parents are aware of and comply with this policy;
- work closely with the Governing Body and the coordinator to create a safe ICT learning environment by having in place:
  - o an effective range of technological tools
  - o clear roles and responsibilities
  - o safe procedures
  - o a comprehensive policy for pupils, staff and parents
- ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- embed e-Safety in all aspects of the curriculum and other school activities;
- provide guidance, support and training to all staff;
- monitor the effectiveness of this policy by:
  - o monitoring learning and teaching through observing lesson
  - o monitoring planning and assessment
  - o speaking with pupils, school staff, parents and governors
- ensure that editorial responsibility of the school Web site is checked and content is accurate and appropriate;
- maintains a log of all online-Safety incidents;

Role of School Staff

School staff will:
- comply with all aspects of this policy
- undertake appropriate training;
- before using any Internet resource in school must accept the terms of the 'Responsible Internet Use' statement;
- not allow others to use their login details;
- report any suspicion or evidence that there has been a breach of security;
- teach pupils the importance of password security;
- not allow others to use their login details;
- report any suspicion or evidence that there has been a breach of security;
- teach pupils the importance of password security;
- be responsible for promoting and supporting safe behaviours with pupils;
- promote online-Safety procedures such as showing pupils how to deal with inappropriate material;
- report any unsuitable website or material to the Headteacher;
- will ensure that the use of Internet derived materials complies with copyright law;
- ensure online-Safety is embedded in all aspects of the curriculum and other school activities;
- make clear their expectations of the children and the importance of a responsible attitude to using the Internet. Internet access will only be possible during supervised teaching

time. Material viewed on the Internet will be appropriate to the curriculum area being covered. Extraneous and irrelevant material will not be included.

Role of Pupils

Pupils will be aware of this policy and will be taught to:

- be critically aware of the materials they read;
- validate information before accepting its accuracy;
- acknowledge the source of information used;
- use the Internet for research;
- respect copyright when using Internet material in their own work;
- report any unsuitable website or material to a member of staff;

Role of Parents/Carers

Parents/carers will:

- be aware of and comply with this policy;
- be asked to support the online-Safety policy and to sign the consent form allowing their child to have Internet access;
- make their children aware of the online-Safety policy;

Internet Use

The school Internet access will:

- be designed for pupil use;
- include school filtering configuration provided and approved by the Head Teacher which is designed to protect pupils;
- provide filtering which is reviewed annually and improved if necessary;
- include filtering appropriate to the age of pupils;
- have virus protection installed which will be updated regularly;
- be reviewed and improved

Curriculum Use of the Internet

There is a clear, progressive e-safety program throughout all Key Stages, built on national guidance.
Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
- to STOP and THINK before they CLICK
- to discriminate between fact, fiction and opinion
- to develop a range of strategies to validate and verify information before accepting its accuracy
- to skim and scan information

- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
- to know how to narrow down or refine a search
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings
- to understand 'Netiquette' behaviour when using an online environment i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- to understand why they must not post pictures or videos of others without their permission

Authorising Internet Access

- Before using any school ICT resource, all pupils and staff must read and sign the 'Acceptable ICT Use Agreement'.
- Parents must sign a consent form before their child has access to the Internet.
- An up to date record will be kept of all pupils and school personnel who have Internet access.

School Website

Contact details on the website will be:

- the school address
- e-mail address
- telephone number

The school website will not publish:

- staff or pupils contact details;
- the pictures of children without the written consent of the parent/carer
- the names of any pupils who are shown;
- children's work without the permission of the pupil or the parent/carer

Social Networking and Personal Publishing

Pupils will not be allowed access:

- to social networking sites except those that are part of an educational network or approved Learning Platform;
- to newsgroups unless an identified need has been approved

Inappropriate Material

- Any inappropriate websites or material found by pupils or school staff will be reported to the Headteacher who in turn will report to the Internet Service Provider.

Internet System Security

- Everyone must be aware that under the Computer Misuse Act 1990 the use of computer systems without permission or for inappropriate use could constitute a criminal offence.
- All computers are to have antivirus software and a filter such as K9.

Complaints of Internet Misuse

- The Headteacher will deal with all complaints of Internet misuse by school staff or pupils.
- Parents will be informed if their child has misused the Internet.

Raising Awareness of this Policy

We will raise awareness of this policy via:

- the school website
- meetings with parents such as introductory, transition, parent-teacher consultations and periodic online-safety workshops
- staff meetings
- information displays in all classrooms (SMART)

Training

All school staff:

- receive training on induction which specifically covers:
    - All aspects of this policy
    - Safeguarding & Child Protection
    - Acceptable Internet Use Agreement
    - Mobile Phone Safety & Acceptable Use
    - Photographic & Video Images
    - Internet Social Networking Websites

Headteacher:		Date:	
Chair of Governing Body:		Date:	

COVID-19 School Closure Arrangements for Online Safety at Shalom Noam Primary School

Context:
With the advent of the Coronavirus pandemic and the closure of schools for the majority of children on 20th March 2020, there has been a shift in schools towards providing online home learning as an efficient way of continuing children's education. This has necessitated a greater use of the internet and web-based resources for both staff and pupils. As time spent on the internet increases, so does the potential for harm. This addendum to the Shalom Noam Primary Online Safety Policy sets out the additional measures and protocols put into place to ensure that children and staff are kept safe whilst working at home.

1. **Online Safety in School**

   Shalom Noam will continue to provide a safe environment, including online. Where pupils are using computers in school, appropriate supervision will be in place.

2. **Children and Online Safety Away from School**

   Online teaching should follow the same principles as set out in Shalom Noam's Staff Code of Conduct and the main Shalom Noam Online Safety Policy.

   Shalom Noam will ensure any use of online learning tools and systems are in line with privacy and data protection/GDPR requirements.

   All procedures and expectations stated in the main Shalom Noam Online Safety Policy must continue to be adhered to.

   Parents will be reminded of the support available to them in order to help to keep their children safe online through the Shalom Noam Newsletter.

   Wherever possible, staff should use school equipment for setting online learning and communications with parents/carers and children.

3. **Home Learning**

   The majority of home learning will be set using Google classroom and zoom lessons

   Children are required to use the code and waiting room to get onto the lessons.

   Children should show their faces on the lessons at all times.

   Where children are directed to alternative websites, for example to access video resources, staff will check the suitability of the content before directing children to access them

   Staff will wear suitable clothing, as should anyone else in their household if recording or videoing, e.g. a story time session for children

   Staff will be mindful of what can be seen in the background if making a recording.

   Language must be professional and appropriate at all times, including any family members in the background.

4. In light of our change in practice due to COVID19, it may be necessary for staff to use their personal mobile phones to communicate with students, parents and carers. Where this is deemed necessary, this must be agreed by a member of the Leadership Team. Where applicable, staff should make sure any phone calls from a personal device are made from a blocked number, so

personal contact details are not visible. Keying 141 before the phone number will block your caller ID on the call you're making.

5. **Reporting Procedures**

   An essential part of the online planning process will be ensuring children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online.