INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) ACCEPTABLE USE POLICY,

INCLUDING CYBER-BULLYING

Legal status

- Based on guidance from the DfE, BECTA and CEOP.

Applies to

- Sacks Morasha Jewish Primary School including the Early Years Foundation Stage (EYFS)
- all staff (teaching and non-teaching), Governors and volunteers working in the school.

Related documents

- Anti-bullying Policy
- Safeguarding – Child Protection Policy
- Safeguarding Children in our School – Guidance for Staff
- Behaviour and Discipline Policy
- Communications Policy.

Availability

This policy is available to parents on request from the school Office. It is also available to staff on the school intranet.

Monitoring and review

- This policy will be subject to continuous monitoring, refinement and audit by the Headteacher.
- The Governors undertake a formal review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than one year from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

The primary purpose of this Acceptable Use Policy is to safeguard pupils and staff at Sacks Morasha Jewish Primary School. It details the actions and behaviour required from pupils and members of staff in order to maintain an e-safe environment and is based on current best practice drawn from a wide range of sources.

For pupils

Pupils at Sacks Morasha Jewish Primary School will be given individual access rights to our computing facilities and will be provided with access to filtered email, internet and other services operating at Sacks Morasha Jewish Primary School.

Internet (www) access (filter controlled)

Having internet access will enable pupils to explore thousands of global libraries, databases and bulletin boards. They will also be able to exchange messages with other learners and teachers throughout the world.

To use this service, pupils will be provided with a unique username and password to enable them to access the network. All unsuitable websites will be filtered and automatically blocked by our security systems and will not be

made accessible to pupils. In addition, pupils' usage of our network will be continuously monitored and repeated attempts to access unsuitable sites will alert our network co-ordinator. The network co-ordinator will tailor the filtering to suit the individual needs of subjects and the school generally. Although this filtering uses the latest security technology, parents will wish to be aware that some pupils may find ways to access material which is inaccurate, defamatory, illegal or potentially offensive to some people.

At Sacks Morasha Jewish Primary School we believe that the benefits to pupils having access to the internet in the form of information, resources and opportunities for collaboration exceed any disadvantages. However, as with any other area, parents and guardians of minors along with Sacks Morasha Jewish Primary School share the responsibility for setting and conveying the standards that pupils should follow when accessing and using these media information sources at school and/or at home. During school time, teachers will guide pupils towards appropriate material on the internet. Outside school, families bear the same responsibility for guidance as they exercise with other information, sources such as television, telephones, films and radio, etc.

ICT-BASED FORMS OF ABUSE (INCLUDING CYBER-BULLYING POLICY)

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

Introduction

Information and communication technology (ICT)-based forms of child physical, sexual and emotional abuse can include bullying via mobile telephones or online (internet) with verbal and visual messages. This annexe focuses on child sexual abuse and bullying. However, the procedure will be followed in other instances of ICT-based abuse e.g. physical abuse (such as, pupils being constrained to fight each other or filmed being assaulted).

Recognition and response

The impact on a child of ICT-based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer, a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family.

All adults (volunteers and staff) working with pupils, adults and families will be alerted to the possibility that:

- a child may already have been/is being abused and the images distributed on the internet or by mobile telephone
- an adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images
- an adult or older child may be viewing and downloading child sexual abuse images.

Chat-room grooming and offline abuse

Our staff will need to be continually alert to any suspicious activity involving computers and the internet. Grooming of pupils online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

E-safety

The Child Exploitation and Online Protection Centre (CEOP) brings together law enforcement officers, specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24-hour online facility for reporting instances of online child sexual abuse. The main concern for teachers is the safe and effective

supervision of pupils using the internet in school.

However, many pupils now use the internet at home for homework and socialising, therefore the staff will need to help the parents understand the positive ways in which the internet can be used, but also some of the associated risks. The website www.becta.org.uk outlines clearly the requirements of a school to control the pupil's internet viewing and instate 'Acceptable Use Policies'.

Cyber-bullying

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

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

Seven categories of cyber-bullying have been identified.

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

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

We will offer parents information sessions on the dangers of cyber-bullying and online child protection issues at regular intervals. Research has found that:

- between a fifth and a quarter of pupils have been cyber-bullied at least once over the previous few months
- phone calls, text messages and email are the most common forms of cyber-bullying
- there is more cyber-bullying outside school than in
- girls are more likely than boys to be involved in cyber-bullying in school, usually by phone

- for boys, text messaging is the most usual form of cyber-bullying, followed by picture/video clip or website bullying
- picture/video clip and phone call bullying are perceived as the most harmful forms of cyber-bullying
- website and text bullying are equated in impact to other forms of bullying
- around a third of those being cyber-bullied tell no one about the bullying.

Sanctions

Each individual case that is in breach of this policy will be dealt with taking into account the severity of the infringement. In extreme cases, the Headteacher might recommend expulsion but other sanctions, for example restriction of access to the school's technology will be considered. Pupils will be expected to sign to agree with the terms of this Policy that will form a part of the School/Pupil/Parent Contract.

For staff

You must not use any ICT on site until you have signed this document and logged it with Personnel.

- I will respect all ICT equipment/facilities at Sacks Morasha Jewish Primary School and will report any faults that I find or any damage that I accidentally cause.
- I agree to abide by this policy in respect of any of my own ICT equipment that I bring on site. The Head or Deputy Head will give permission to bring home owned ICT devices on site but this permission may be withdrawn on an individual basis. If any ICT device is being used inappropriately or illegally on site, the Head or Deputy Head may request that the device be monitored. Failure to give permission may result in withdrawal of permission to bring the device on site and informing of the appropriate authorities.
- I am familiar with the school's Data Protection Policy and I agree I am responsible for the security of all personal data in my possession. I agree that all personal data that relates to an identifiable person and is stored or carried by me on a removable memory device will be encrypted or contained within password-protected files to prevent unauthorised access.
- I am responsible for my use of my own log-in details and if I suspect that my log-in details have become known to others then I will immediately ask for these details to be changed.
- I agree that my use of Sacks Morasha Jewish Primary School ICT equipment/facilities will be monitored and may be recorded at all times. I understand that the results of such monitoring and recording may be shared with other parties if I break the terms of this Acceptable Use Policy.
- I will not deliberately attempt to access any unsuitable websites, services, files or other resources when on site or using Sacks Morasha Jewish Primary School equipment/facilities. I understand that I may temporarily access blocked websites, services and other online resources using only tools that are provided by Sacks Morasha Jewish Primary School. I agree that I will not display blocked websites, services and other resources to others until I have fully assessed the materials and have found them to be entirely suitable for the intended audience.
- I agree that the provision of Sacks Morasha Jewish Primary School ICT equipment/facilities are for educational purposes although limited personal use is permitted provided that this is not done during normal working time and does not contravene any of the other clauses in this document.
- I am aware that downloading copyright materials, including music and video files without paying the appropriate licence fee is often a criminal act. I am aware that any involvement in criminal acts relating to the use of ICT on site or using Sacks Morasha Jewish Primary School equipment/facilities may result in disciplinary or legal action. I will not deliberately engage in these acts.
- I will not deliberately view, send, upload or download any material that is unsuitable for the school environment whilst I am in that environment or using any ICT equipment/facilities belonging to Sacks Morasha Jewish Primary School. If I accidentally encounter any such material then I will immediately close, but not

delete in the case of emails, the material and report it to the e-Safety co-ordinator or to a senior member of staff. I will not be penalised if I view unsuitable material accidentally and by reporting such incidents I will help to improve e-Safety. If I am in any doubt about the suitability of any material, or if a colleague raises any doubts, then I will not (re)access the material without the agreement of the e-Safety co-ordinator. I will not access any material that the e-Safety co-ordinator has rated as unsuitable.

- Unless specifically authorised to do so, I will not disclose any of my personal details, other than those that identify me professionally, nor log any such details on websites whilst using Sacks Morasha Jewish Primary School equipment or facilities. If I disclose any additional personal details contrary to this instruction then I agree that these details can be recorded and that I will not hold Sacks Morasha Jewish Primary School responsible for maintaining the security of the details I have disclosed.
- I agree that professional standards of communication will be maintained at all times when using equipment or facilities of Sacks Morasha Jewish Primary School.

I understand all of the above.

Signature _____

Print name _____

Date _____

Reviewed by Headteacher – Hayley Gross July 2020