Policy on **E-Safety**

November 2024

Pardes House Primary School

Headteacher: Rabbi J Sager

POLICY ON E-SAFETY

Partnership

This policy is the culmination of work between the school's Headteacher, Religious Principal, Chair of Governors and head of the school's religious body.

Scope of the policy

This policy applies to all members of the *school* (including staff, pupils, volunteers, parents, visitors and any community users) who have access to and are users of school IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of 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 outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Introduction

Technology and communications are rapidly changing and becoming more sophisticated. With this change comes new ways of being unsafe and feeling threatened. E- Safety has become a very important issue that is essential to address in school, to ensure that all children and adults remain safe and in control when using technology. This could be either computers, smart-pads or having access to the internet and/or through mobile telephones.

Aims

- While the school makes use of modern technologies, we aim to ensure that our children do not have access to technologies where there is the possibility of it affecting them negatively and not in a way expected of Pardes House pupils.
- That our staff should know how to use the internet correctly, without misuse.
- That personal information should be kept private.
- To ensure that the necessary measures are taken to block and delete accounts, messages and people, where necessary.

Roles and Responsibilities

All adults involved in the life of the school; whether governors, teaching staff, support staff, technicians have roles and responsibilities associated with E-Safety.

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 receiving regular information about e-safety incidents, filtering and monitoring reports. The Governor responsible for Safeguarding is also the E-Safety Governor. The role of the E-Safety Governor will include:

- Termly meeting with the Headteacher.
- Regular monitoring of e-safety incident logs and filtering monitoring reports.
- Reporting to relevant Governors as needed.
- Reviewing annual online safety review with the Headteacher

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community
- The Headteacher (Designated Person for Child Protection) is aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that relevant staff receive suitable training to enable them to carry out their e-safety roles.
- The Headteacher will take day-to-day responsibility for e-safety issues.
- The Headteacher will receive reports of e-safety incidents and of issues relating to the filtering applied by the network.
- The Headteacher will be responsible for creating a log of incidents, to inform future e-safety developments.
- The Headteacher will meet with Governors as required to discuss current issues, review incident logs and filtering / change control logs and reports regularly to Senior Leadership Team.
- The Headteacher liaises with the Local Authority where necessary.
- The Headteacher and other senior leaders will liaise with school technical staff.
- The Headteacher will carry out monthly filtering checks.
- The Headteacher will carry out an annual online safety review.

Computing Leader, E-Safety Leader & Technical staff
Are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e-safety technical requirements.
- That users may only access the networks and devices through a properly enforced password protection system.
- That they keep up to date with e-safety technical information and update others as relevant.
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse.
- That the school's filtering systems are maintained and effective.

Filtering and Monitoring
The school is responsible for ensuring that its network is as safe and secure as is reasonably possible and that correct procedures are implemented. It will also need to ensure that the

relevant people named above will be effective in carrying out their monitoring responsibilities:

- School IT systems will be managed in ways that ensure that the school meets online-safety requirements and any relevant guidance.
- Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will be provided with a username and password.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service.
- In the event of a need 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.
- 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 Headteacher and Computing Leader. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.
- The Headteacher will carry out half-termly filtering checks.

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 report any suspected misuse or problem to the Headteacher for investigation / action / sanction.
- All digital communications with parents should be on a professional level and only carried out using official school systems.
- Pupils understand and follow instructions re. e-safety.
- Monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned, sites should be checked as suitable for use and if unsure, checked with the Headteacher or Computing Leader.

Designated Person for Child Protection

Has been trained in e-safety issues and is aware of the potential for serious child protection / safeguarding 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.

E-Safety and risk of radicalisation

From 1st July 2015, all schools became subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have "*due regard to the need to prevent people from being drawn into terrorism*". This duty is known as the Prevent Duty (DfE 2015).

There are four key duties for schools: Identify local risks, identify at risk students, work in partnership with other agencies and keep children safe online, where much of the radicalisation takes place. The Prevent duty applies to all schools.

Regarding radicalisation and e-safety, at Pardes House, we ensure that children are safe from terrorist and extremist material if they access the internet in school. The school has suitable filtering is in place via the London Grid for Learning.

Pupils

- Are responsible for using the school digital technology systems responsibly;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Will be expected to know and understand acceptable use of digital cameras;
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events;
- The school website.

Parents will also be invited to e-safety evenings, led by school staff and external facilitators.

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore 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 curriculum is taught annually as part of the Computing curriculum and for keeping children safe.
- Key e-safety messages may be reinforced as part of the school's assembly programme.
- Pupils will be helped to understand the need for the pupil acceptable use and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

Education – parents

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and

young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents through:

- Curriculum activities;
- Letters, newsletters, website;
- Parent e-safety workshops;
- Reference to the relevant websites / publications.

Technical Notes

- 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:
- Pardes House Primary School receives a filtered broadband service through the London Grid for Learning. Amongst other things, this service is intended to stop users from accessing any material that would be regarded as inappropriate for the learning environment or illegal.
- The school still has ownership of what else needs to be filtered as technology advances.
- All staff will be made aware that there is a monitoring and filtering system in place and any online activity can be traced. The person responsible for monitoring this will also be monitored by the Headteacher to ensure that this is being done effectively and correctly.
- All personal data will be stored accordingly to the Personal Data Act 1998. Staff must use personal data on secure password protected machines and other devices, ensuring that they 'log off' at the end of any session. This will then minimise any chance of the data being seen by others. Any personal data that is stored on a USB device also needs to be password protected an encrypted. Devices must have virus and malware checking software. Any data must be securely deleted from any devices.
- The school's technical computer systems are managed with the support of an external computer support company.

Use of digital and video images

Please see separate policy relating to use of cameras and mobile phones in school.

Social Networking

Social networking sites, such as Instagram, TikTok, SnapChat and Facebook provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.
- Staff are not allowed to befriend pupils on any social networking sites and should inform the Headteacher if a child tries to do so.
- Any member of staff who does not meet this expectation will be subject to a disciplinary investigation as per the Code of Conduct.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment.

School staff should ensure that:

- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

Video conferencing will not be used without due consideration by senior leaders.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a decision made on their use by the Headteacher.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that the school must ensure that information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

The school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

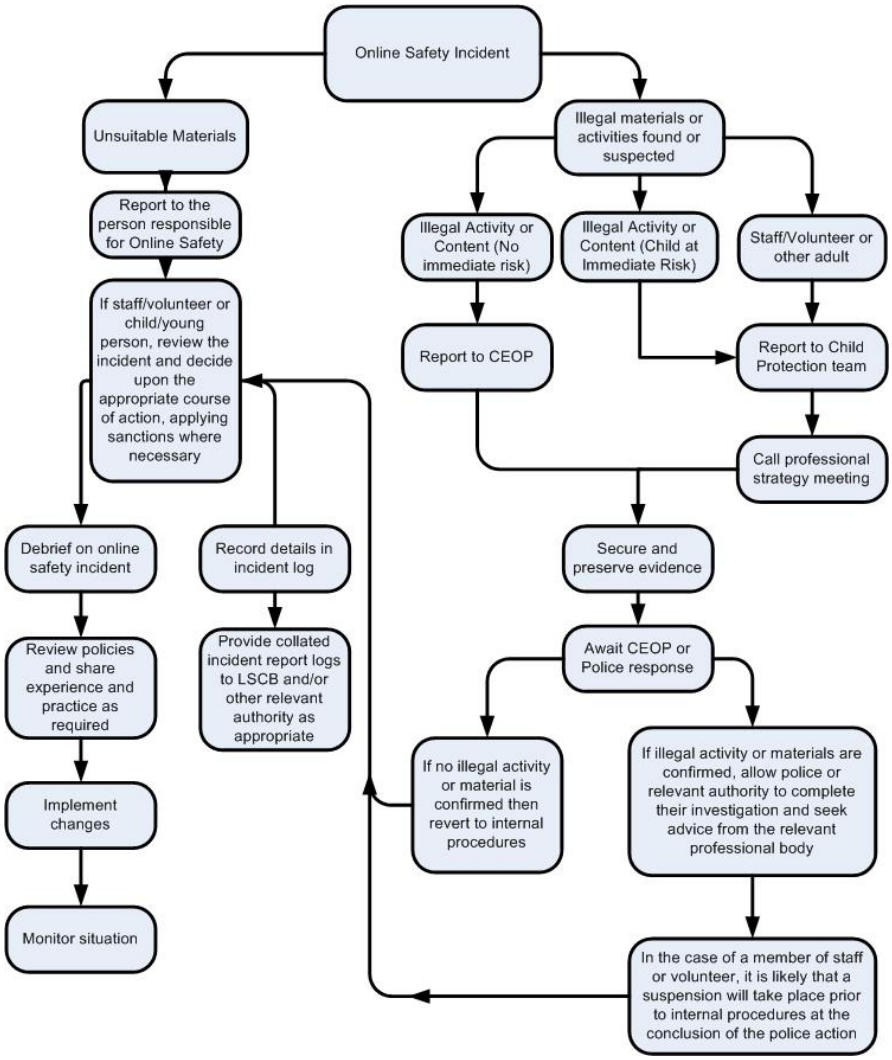
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- It has a Data Protection Policy.
- Responsible persons are appointed / identified.
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.

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 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.
- Transfer data using encryption and secure password protected devices.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (next page) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is expected that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the 'url' of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).

Once this has been completed and fully investigated, a judgement will be made whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures;
- Involvement by Local Authority or national / local organisation (as relevant);
- Police involvement and/or action.

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- Incidents of 'grooming' behavior;
- The sending of obscene materials to a child;
- Adult material which potentially breaches the Obscene Publications Act;
- Criminally racist material;
- Other criminal conduct, activity or materials.

The computer in question will be isolated. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that

incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupils

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X			
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users				X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Continued infringements of the above, following previous warnings or sanctions		X		X				X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X				X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X		X	X

Actions / Sanctions

Staff

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X		X		X			X
Inappropriate personal use of the internet / social media / personal email	X		X				X	
Unauthorised downloading or uploading of files	X					X	X	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X					X	X	
Careless use of personal data eg holding or transferring data in an insecure manner	X						X	
Deliberate actions to breach data protection or network security rules			X			X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software			X			X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X	X	X			X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils			X	X				X
Actions which could compromise the staff member's professional standing			X	X				X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X					X
Using proxy sites or other means to subvert the school's filtering system	X						X	X
Accidentally accessing offensive or pornographic material and failing to report the incident			X	X				
Deliberately accessing or trying to access offensive or pornographic material					X			X
Breaching copyright or licensing regulations			X					X
Continued infringements of the above, following previous warnings or sanctions			X					X

Reference and further information can be found on the following websites:

www.thinkuknow.co.uk

www.disrespectnobody.co.ukwww.saferinternet.org.uk www.internetmatters.org

www.childnet.com/cyberbullying-guidance www.pshe-association.org.uk

http://educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-onlineradicalisation
www.gov.uk/UKCCIS

_____

Date: November 2024 Review: November 2026