Hassocks Infant School

E-Safety Policy

✭ Explore ✭ Respect ✭ Flourish

Date policy agreed:	November 2021
Date policy to be reviewed:	November 2025
Responsibility:	Head Teacher Safeguarding Link Governor

Contents

1. Introduction 3
2. Responsibilities 3
3. Scope of policy 3
4. Policy and procedure 4
    Use of email 4
    Visiting online sites and downloading 5
    Storage of Images 6
    Use of personal mobile devices (including phones) 6
    Reporting incidents, abuse and inappropriate material 7
5. Curriculum 8
6. Staff and Governor Training 8
7. Working in Partnership with Parents/Carers 9
8. Records, monitoring and review 9
Appendices to this policy: 10

1. Introduction

Hassocks Infant School recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

2. Responsibilities

The Headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead is the Designated Safeguarding Lead (DSL). Deputy Designated safeguarding leads will assume responsibility in the absence of the Designated Safeguarding Lead.

All breaches of this policy must be reported to the DSL.

All breaches of this policy that may have put a child at risk must also be reported to the DSL or Deputy DSL.

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount and the organisation must adhere to the school's online safety procedures, acceptable use agreements and safeguarding policies.

3. Scope of policy

The policy applies to:

- ☆ pupils
- ☆ parents/carers
- ☆ teaching and support staff
- ☆ school governors
- ☆ peripatetic teachers/coaches, supply teachers, student teachers
- ☆ visitors
- ☆ volunteers
- ☆ voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, regular updates in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents including: Child Protection, Keeping Children Safe in Education, GDPR, Health and Safety, home–school agreement, Homework, Behaviour, staff handbook and code of conduct and PSHE/RSE policies.

4. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and governors should use a school email account for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to the Designated Safeguarding Lead so that these can be investigated.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Children do not have access to email accounts. We recognise the value of teaching children to send emails and this can greatly enhance the curriculum. Any emails sent to external recipients will be closely supervised by the class teacher, for example by writing a collaborative email using the large display in the classroom. Class teachers should check class inboxes for inappropriate content in advance of a lesson and before this is displayed to the class. Children will be supervised at all times. Any emails sent on Purple Mash as part of the school's computing curriculum are monitored by the class teacher and Computing leader.

Visiting online sites and downloading

Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Head Teacher with details of the site/service and seek approval. Staff should not sign up to online services without prior consent. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research or an online task is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.

Staff must only use pre-approved systems if creating blogs, wikis or other online content. Wherever possible, staff should make use of Purple Mash which is a closed system which is monitored by staff.

When working with pupils searching for images should be done through Google Safe Search, Google Advanced Search or a similar application that provides greater safety than a standard search engine. Careful consideration should be given to any key words used for searches and children should be supervised at all times when searching the internet.

Users must not:
Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse; (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18; (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK;
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation;
- Promoting hatred against any individual or group from the protected characteristics above;
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy;
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect;

Any instances in breach of these rules must be reported to a Designated Safeguarding Lead immediately. The Designated Safeguarding Lead will follow procedures in our safeguarding policy. Any illegal acts must be reported to the police immediately.

Users must not:

- Reveal or publicise confidential or proprietary information;
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses;
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to

the school;

- ☆ Use the school's hardware, internet access and Wi-Fi facilities for running a private business;
- ☆ Intimidate, threaten or cause harm to others;
- ☆ Access or interfere in any way with other users' accounts;
- ☆ Use software or hardware that has been prohibited by the school;

Teaching staff are provided with laptops to use outside of school. Wherever possible, school devices should be used to conduct school business outside of school, unless a closed, monitorable system is used. Such a system would ensure the user was not saving files locally to their own device and breaching data security.

A monitorable system would be one such as the school's Remote Desktop service or Office 365. Any school documents access through remote services should not be downloaded to the local device. Users should log out of the Remote Desktop or Office 365 at the end of the session. School devices provided for home use should only be used by staff and are should not be used by family members.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police or Local Authority Designated Officer (LADO).

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR, they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to approved staff as determined by the school.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren. The school will remind families of this expectation at events, for example Christmas performances.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. Personal devices, such as mobile phones or tablets should not be used. See also GDPR.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Designated areas include:

- ☆ Staff room

- ☆ PPA room
- ☆ Designated office spaces

There may be some, occasional exceptions to this guidance which may necessitate using a mobile phone during the school day. This includes an emergency situation where it is not possible to access school telephones, e.g. the school field.

Staff may use phones in shared spaces at the start and end of the school day when pupils are not on-site. When children are on-site, phones should be switched off or put into silent mode and stored out of sight from pupils.

Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device. Due to the age of pupils in our school, staff members should never contact a pupil directly - contact will always be made through parents.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the school. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off or in silent mode and out of sight.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider the educational benefit and carry out a risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with a senior leader before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, a DSL or the Head Teacher. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to the Integrated Front Door (IFD) or the police.

The school does not tolerate cyber-bullying and incidents will be investigated by a senior leader. The school will follow the school's behaviour policy or staff disciplinary policy when dealing with confirmed incidents of cyber-bullying.

Staff members should use CPOMs to report any concerns, in line with safeguarding procedures.

5. Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. The PSHE curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education. This includes teaching at an age appropriate level to prevent radicalisation, for which staff provide a narrative to counter extremism.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- ☆ Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity;
- ☆ Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment;
- ☆ Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives;
- ☆ Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online;
- ☆ Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others;
- ☆ Understanding the permanency of all online postings and conversations;
- ☆ Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images;
- ☆ Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help;
- ☆ How the law can help protect against online risks and abuse;

Content will be delivered in an age-appropriate context, relevant to the age of the child and in response to individual needs.

6. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of whole school training records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children and based on the school premises are also provided with a copy of the online safety policy.

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (see appendices)

Guidance is provided for occasional visitors, volunteers and parent/carer helpers as part of the safeguarding induction process. (see appendices)

7. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and parent workshops.

Parents/carers are asked to read, discuss and co-sign with each child the Acceptable Use Agreement on admission to the school. A summary of key parent/carer responsibilities will also be provided and is available in (see appendices). The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported on CPOMS.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

The safeguarding governor will receive regular updates on the implementation of this policy and E-Safety incidents during termly link governor meetings with the DSL.

Appendices to this policy:

- Staff Acceptable Use Policy Agreement
- Pupil Acceptable Use Policy Agreement
- Internet letter to parents / carers
- User agreement and parental permission form for Internet access
- Rules for staying safe on the Internet (guidance for classrooms)
- Permissions form