DATE PALM
PRIMARY
Building foundations for life

E-SAFETY POLICY

DATE PALM STATEMENT of INTENT

At Date Palm our vision is for the School to ensure our pupils grow like a Date Palm tree – with **strong foundations, lofty branches and produce fresh fruit**:

- ✓ To build **Strong Foundations for Character Development** that:
  Instil values; inspire each pupil; display best manners.
- ✓ To have **Lofty Branches of Educational Excellence** that will:
  Provide a broad and varied range of experiences and learning opportunities; help each pupil progress and develop in all aspects; support their skills and talents.
- ✓ To produce **Fresh Fruit that provides services to their Communities** in order to:
  Become responsible and confident citizens; make a positive difference; commit to charitable endeavours; become effective contributors towards Britain's future.

Reviewed by	Position	Signature
Saira Karim	E-Safety Coordinator	S.Karim
Sabina Yesmin	Safeguarding Governor	S.Yesmin

Reviewed: November 2022
Next review date: November 2023

DATE PALM
PRIMARY
Building foundations for life

E- Safety Policy

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Our E-safety Policy has been written by the school, following government guidance. This policy is written in line with the requirements of:

- Keeping Children Safe in Education 2022
- Relationships Education, Relationships and Sex Education (RSE) and Health Education 2019

Introduction

The resources used by pupils in school are carefully chosen by the teachers and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information, which has sometimes not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times they will be able to move beyond these to sites unfamiliar to the teacher. There is therefore the possibility that a pupil may access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the internet.
- Describe how these fit into the wider context of our behaviour and PHSCE policies.
- Demonstrate the methods used to protect the children from sites containing unsuitable material.

The school believes that the benefits to pupils from access to the resources of the internet far exceed the disadvantages. Ultimately the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

At Date Palm, we feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Parents will be sent an explanatory letter and the rules, which form our Internet Access Agreement (Attached to the end of this document). This will form part of our pupil registration welcome pack. We will also aim to disseminate any relevant published materials to parents.

Roles and Responsibilities of Governors

Governors are responsible for the approval of the E-Safety policy and for reviewing the effectiveness of the policy. The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Coordinator
- Regular monitoring of E-safety incidents

Head teacher and Senior Leaders

- The senior leadership team are responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Coordinator.
- The Head teacher is responsible for ensuring that the E-safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Head teacher and Deputy head should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The E-Safety Coordinator

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school's e-safety policy.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.

Teaching and Learning

The internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality internet access as part of their learning experience:

- The school internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- All key stages will focus on different elements of staying safe online. These units include topics from how to use a search engine, digital footprints and cyber bullying.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband network including the effective management of filtering.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings with our

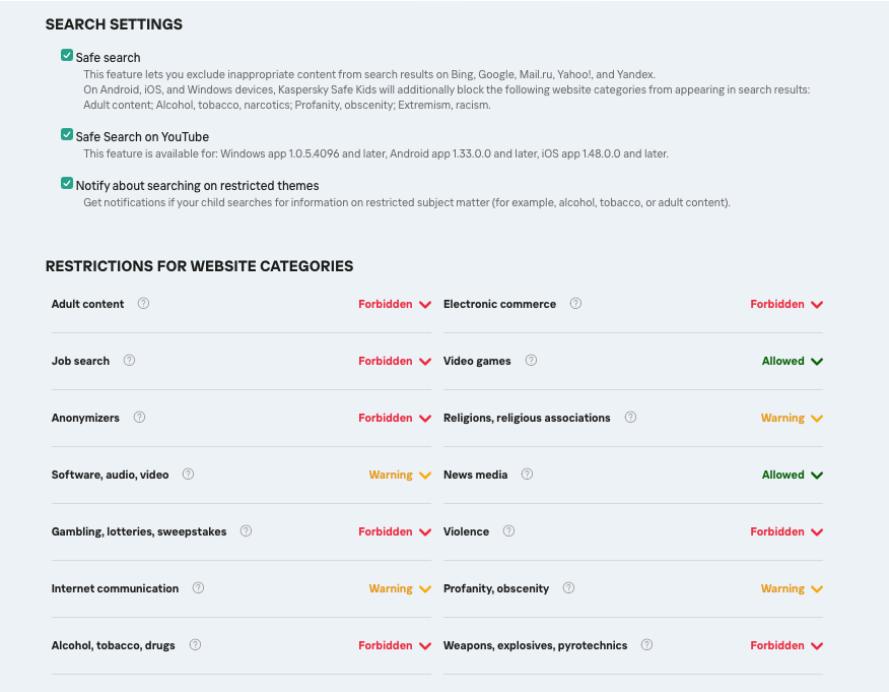
SEND coordinator and individual teachers to ensure all children have equal access to succeeding in this subject.

Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.

World Wide Web

The internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework and sharing ideas are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Head teacher, by recording the incident in an e-Safety Log, which will be stored in the Head teacher's office with other safeguarding materials. The e-Safety Log will be reviewed termly by the e-Safety Co-ordinator.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.



Internet content will be filtered for all users (students, teachers, administrators) as shown above.

Email

Email is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.
- Whole class or group email addresses should be used in school, individual addresses should never be used.
- Access in school to external personal email accounts is not allowed.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as using outlook.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Security and passwords

Passwords should be changed regularly. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC with a screen saver if they are going to leave it unattended (the picture mute or picture freeze option on a projector/smart board will allow an image to remain on the screen and also allow a PC to be 'locked').

Social Networking

Social networking internet sites (such as, MySpace, 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.

Reporting

All breaches of the e-safety policy need to be recorded in the E-Safety reporting book that is kept in the Head Teacher's office. Copies of the log are kept in each classroom too for quick access. The details of the user, date and incident should be reported on the log.

Incidents which may lead to child protection issues need to be passed on to the Designated Safeguarding Office immediately – see Safeguarding Policy.

Allegations involving staff should be reported to the Head teacher - See Safeguarding Policy.

Mobile Phones

Many new mobile phones have access to the internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the internet and sharing of images. There are risks of mobile bullying, or inappropriate contact. Only in exceptional circumstances children will be allowed to have a mobile phone e.g. for safety before or after school. Mobiles should be handed to the school office as soon as the child is in the school.

- Staff should always use the school phone to contact parents.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.
- Staff may use their mobile phones in the staffroom.
- Parents cannot use mobile phones on school trips to take pictures of the children.
- School mobiles will be used on trips. Staff will not take personal mobiles with them.

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the internet, but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.
- The Head teacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos is not permitted.
- Staff should always use a school camera to capture images and should not use their personal devices.
- Photos taken by the school are subject to the Data Protection Act & GDPR legislation 2018.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the website will be the school address, email and telephone number.
- Staff and pupils' personal information will not be published.
- The Head teacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school website.
- Parents should only upload pictures of their own child/children onto social networking sites.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998, Freedom of Information Act and GDPR 2018. (See GDPR policy)

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Unacceptable use of ICT and the internet

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language online
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Senior Leadership Team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Handling E-Safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures. See Safeguarding policy.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies.

Communication of Policy

Pupils:

- Pupils will be informed that internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites. This will be strongly reinforced across all key stages during Computing lessons.

Staff:

- All staff will be given the School E-safety Policy and its importance explained.

Parents:

- Parents' will be provided access to the schools E-safety policy, other guidance on internet safety and will also be asked to sign the internet access agreement form.

Further Resources

We have found these web sites useful for e-safety advice and information.
http://www.childnet-int.org/

http://www.thinkuknow.co.uk/

APPENDIX A

All Parents are asked to sign the acceptable use agreement form:

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students* will have good access to digital technologies to enhance their learning and will, in return, expect the *students* to agree to be responsible users. A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to give written permission using the example below to show their support of the school in this important aspect of the school's work.

Parent / Carer Permission Form

I understand that the school has discussed the Acceptable Use Agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Please insert the names of yourself and your child.

I, (insert full name of parent) _____ agree to the 'Parent/Carer Acceptable Use Agreement' and give permission for my child, (insert child's full name) _____ to have access to the internet and to ICT systems at school.

APPENDIX B

KS2 children are asked to sign the acceptable use agreement form:

Pupil Acceptable Use Agreement

When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Use chat rooms
- Use a personal email address when emailing in school
- Email people I don't know unless a teacher has approved it.
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Share my password with others or log in using someone else's name or password
- Give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends.
- Look at other people's files without their permission.
- Use school devices for online gaming, file sharing or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- Bully other people

I understand that the school will check emails and the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will use the school's computers with care, ensuring I do not damage them through carelessness or inappropriate use. I will report all damages or faults to an adult immediately. I understand that the school can remove my ICT privileges if I do certain unacceptable things online, even if I'm not in school when I do them.
Date:
Signed (pupils):

APPENDIX C

Staff, trustees, volunteers and visitors who use the school's ICT facilities or internet are asked to sign the acceptable use agreement form:

Staff, Trustees, Volunteers & Visitors Acceptable Use Agreement

Name of staff member/trustee/volunteer/visitor:
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Use any improper language when communicating online, including in emails or other messaging services • Accept invitations from children or young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. • Use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school
I understand that the school can monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance

with this policy and the school's data protection policy. I will ensure that I log off all apps and devices after my network session has finished. I will let the designated safeguarding lead (DSL) and SLT know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed:	Date:

APPENDIX D

E-safety incident report form

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

□ online 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

□ **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

□ disciplinary action to be taken

□ e-safety policy to be reviewed/amended

Please detail any specific action taken

□ **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

□ child's parents informed

□ disciplinary action to be taken

□ child/young person debriefed

□ e-safety policy to be reviewed/amended

Outcome of incident/investigation