Online Safety Policy

These guidelines are for the whole school, including EYFS

Key Details:

The Dharma Primary School Designated Safeguarding Leads are:

Head Teacher	Clare Eddison (Primary DSL)
Head of Early Years	Alison Mayo (Deputy DSL)
Deputy Head of Early Years	Mei Mei Jacklin (Deputy DSL)
Trustee with responsibility for safeguarding	Lynne Weir

1. Introduction

The Internet is an essential element in 21st Century life for education, business and social interaction. At the Dharma Primary School we have a duty to provide children with quality internet access as part of their learning experience, whilst ensuring that their welfare is promoted.

In addition, safeguarding (therefore online safety and safeguarding online) and promoting the welfare of children is a responsibility for all members of staff. All school staff have a responsibility to provide a safe environment in which children can learn and this includes the online environment.

This policy has been written with regard to the DfE statutory guidance "Keeping Children Safe in Education" (2019), Early Years and Foundation Stage Framework (revised 2017), new guidance on Relationships and Health Education (2019) and Working Together to Safeguard Children (2018).

This policy is to be read in conjunction with the following: the Child Protection and Safeguarding Policy, Acceptable Use Policy, PSHE Policy, the Anti-bullying Policy, Behaviour Policy, the Social Media Guidelines, the Data Policy and the Code of Conduct. These can be found on the school drive in the folder, 'All School Policies 2020'.

2. Aims and Objectives

The purpose of internet usage in school is to raise educational standards, to promote pupil achievement and to support the professional work of staff.

The purpose of this policy is to:

- Safeguard and protect all members of The Dharma Primary School community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards when using technology.
- Identify clear procedures to use when responding to online safety concerns.

From KCSIE, 2019, '*The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation; technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.'*

The Dharma Primary School recognises that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

3. Scope of Policy

The Dharma Primary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.

The Dharma Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

The Dharma Primary School believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.

This policy also applies to such use off school premises if the use involves pupils or any member of the School community or where the culture, ethos or reputation of the School are put at risk.

4. Roles and Responsibilities

The school has appointed the Primary Designated Safeguarding Lead, DSL, (see above) to be the online safety lead. Furthermore, the two DDSL's role also encompasses online safety and safeguarding.

All members of the school community have important roles and responsibilities concerning online safety.

4.1 The Head, Bursar, DSL's and Trustees will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including the Code of Conduct and Acceptable Usage Policy.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and updated on a regular basis.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Ensure the Designated Safeguarding Leads have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, where possible, evaluating online safety practice to identify strengths and areas for improvement.

4.2 Technical staff will:

- Implement appropriate security measures *(including password policies and encryption)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Report any filtering breaches to the DSL and/or senior leadership team, as well as to the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

4.3 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.

- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the Trustee Body.
- Review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet termly with the trustee with a lead responsibility for safeguarding.

4.4 All members of staff will:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable usage policy (AUP).
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.5 Pupils will: (at a level that is appropriate to their individual age, ability and vulnerabilities)

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

We have an expectation that:

4.6 Parents and carers will:

- Read and abide by the school acceptable usage policy and encourage their children to adhere to it.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Be a role model, through safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school online safety policy.
- Use school online systems safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Introduction

Online or cyberbullying is bullying that takes place using technology. There are many types of online bullying. Examples are:

- Text messages that are threatening or cause discomfort
- Pictures/videos via mobile phone cameras – images sent to others to make the victim feel threatened or embarrassed.
- Mobile phone calls – silent calls or abusive messages, stealing victim's phone and using it to harass others, to make them believe the victim is responsible.
- Emails – threatening or bullying emails, often sent using pseudonym or someone else's name.
- Chatroom bullying – menacing or upsetting responses to children or young people when they are on the web
- Instant messaging – unpleasant messages sent while children conduct real time conversations using MSN or Facebook Chat
- Bullying via websites and gaming sites – use of defamatory blogs, personal websites and social networking such as Facebook.

One of the main aims of this policy is to educate pupils about the risks of online bullying, to prevent, as far as practicable, their present and future engagement with it.

5.2 Education and engagement with pupils

We will establish and embed a progressive online safety curriculum throughout the school, to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in the PSHE and ICC programmes of study, covering use both at home and at school.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The school will support pupils to read and understand Acceptable Usage in a way which suits their age and ability by:

- Displaying acceptable use posters in all teaching rooms.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology by pupils.
- Implementing appropriate peer education approaches.
- Providing online safety education and training as part of transition across the key stages
- Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.

- Using support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches, for instance, Safety Net.

5.3 Vulnerable Pupils

The Dharma Primary School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

The Dharma Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils. We will seek input from specialist staff as appropriate, including the SENCo, Individual Needs Assistants and the SEN Teaching Assistant.

5.4 Training and engagement with staff

The school will:

- Provide and discuss this online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates, as part of overall Safeguarding training.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with the school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

5.5 Awareness and engagement with parents and carers

The Dharma Primary School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.

The school will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as pujas, parent evenings, transition events, fayres and sports' days.
- Drawing their attention to the school's online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our school, for example, within our home-school agreement.
- Requesting them to read the school's AUP (Acceptable Usage Policy) and discuss its implications with their children.

6. Reducing Online Risks

The Dharma Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.

All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

The Dharma Primary School uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Email
- Digital cameras, web-cams and video cameras

All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.

- All devices will have a triple layer of content filtering applied to them.
- All devices will have their browsing history logged.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

The school will use age appropriate search tools, following an informed risk assessment, to identify which tool best suits the needs of our community – Google Safe search is implemented
The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.

Supervision of pupils will be appropriate to their age and ability.

- **Early Years Foundation Stage and Key Stage 1**
    - Pupils' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils' age and ability.

- **Key Stage 2**
    - Pupils will use age-appropriate search engines and online tools.
    - Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

7.2 Managing Internet Access

The school will record users who are granted access to the school's devices and systems.

All staff and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet.

8. Filtering, Monitoring and Management

8.1 Decision Making

- The Dharma Primary School governors and senior leadership team (SLT) have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and SLT are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the Head; all changes to the filtering policy are logged and recorded.
- The SLT will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

8.2 Filtering

- The school uses educational broadband connectivity through (Plus Net)
- The school uses (OpenDNS and PlusNet) which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list.

- The school works with (OpenDNS and PlusNet)) to ensure that our filtering policy is continually reviewed.

Dealing with Filtering breaches

The school has a clear procedure for reporting filtering breaches.

- If pupils discover unsuitable sites, which present a safeguarding risk, they will be required to **turn off monitor/screen and report the concern immediately to a member of staff**.
- The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and to technical staff.
- The breach will be recorded and dealt with as appropriate.
- Parents/carers will be informed of filtering breaches involving their child – subject to safeguarding concerns.

Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Sussex Police or CEOP. If there is a safeguarding concern, the matter will be referred to FDFF and/or the police, following the Child Protection and Safeguarding Policy.

8.3 Monitoring

The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by the IT staff reviewing the internet logs weekly.

The school has a procedure for responding to concerns identified via monitoring approaches. All users will be informed that the use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

8.4 Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation.

8.5 Security and Management of Information Systems

The school takes appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on the school's network.
- The appropriate use of user logins and passwords to access the school network.

    - [Specific user logins and passwords will be given to all but the youngest users. (**For Early Years and Foundation Stage children**)]

- All users are expected to log off or lock their screens/devices if systems are unattended.
- Further information about technical environment safety and security can be found in the AUP.

8.6 Password policy

All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.

From Year 2, all pupils are provided with their own unique username and private passwords to access school systems; pupils are responsible for keeping their password private.

We require all users to:

- Use strong passwords for access into our system.
- Change their passwords every year.
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

8.7 Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

8.8 Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with associated policies, including (but not limited to): the Child Protection and Safeguarding Policy, the Data Policy, the AUP, the Code of Conduct (including the Social media guidelines).

8.9 Managing Email

Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including the AUPs and the Code of Conduct.

- The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.

- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the school community will immediately tell the DSL or a DDSL if they receive offensive communication, and this will be recorded in the school safeguarding log.

Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in school.

8.10 Educational use of Videoconferencing and/or Webcams

The Dharma Primary School recognises that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.

- All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.
- Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
- Video conferencing contact details will not be posted publicly.
- School videoconferencing equipment will not be taken off school premises without prior permission from the DSL.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

- **Users**
  - Parents and carers consent will be obtained prior to pupils taking part in videoconferencing activities.
  - Pupils will ask permission from a teacher before making or answering a video conference call or message.
  - Videoconferencing will be supervised appropriately, according to the pupils' age and ability.
  - Video conferencing will take place via official and approved communication channels following a robust risk assessment.
  - Only key administrators will be given access to videoconferencing administration areas or remote control pages.
  - The unique log- on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely to prevent unauthorised access.

- **Content**

- When recording a video conference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, the school will check that recording is permitted to avoid infringing third party intellectual property rights.

9. Acceptable usage (please see the Acceptable Usage Policy – AUP)

Unacceptable use of digital devices or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material.

In any cases giving rise to safeguarding concerns, the matter will be dealt with by following procedures in the School's Child Protection and Safeguarding Policy.

The IT equipment that the children will have access to is Google Chromebooks. The access they have will be monitored by a member of staff. There is a generic log-in for each Chromebook that is managed by staff. Through this log-in the children will only be able to access accepted websites. The accepted websites on every Chromebook are to be found in the Scheme of Work for ICC and is age-related. There is an email address for children's work which should be used in order for that work to be printed; childrenswork@dharmaschool.co.uk.

Only a member of staff will be able to add acceptable websites through the supervising account. Other accepted sites may be added for specific reasons or uses. Use of school computers by pupils must be in support of the aims and objectives of the school and the National Curriculum. Although at The Dharma Primary School we do our utmost to ensure that the children's access and experience with ICC equipment is a positive and safe experience we have to acknowledge that no filtering systems are one hundred percent effective. Any negative or worrying internet usage with be dealt with in accordance with our safeguarding policy.

9.1 Online activities which are encouraged include:

- The use of email and computer conferencing for communication: between colleagues, between pupils(s) and teacher(s), between pupils, between schools and industry.
- Use of the Internet to investigate and research school subjects, cross-curricular themes or topics related to social and personal development.
- The development of pupils' capabilities in ICC skills and their general research skills.

9.2 Online activities which are not permitted include:

- Searching, viewing or retrieving materials that are not related to the aims of the curriculum.
- Copying, saving or re-distributing copyright-protected material, without approval.
- Subscribing to any services or ordering and goods or services, unless specifically approved by the school.
- Playing computer games or using other interactive 'chat' sites unless specifically approved by the school.
- Using the network in such a way that the use of the network by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages).
- Publishing, sharing or distributing any personal information about a use (such as: home address; email address; phone number; etc).
- Downloading software and screensavers unless given specific permission by the school.

- Any activity that violates the school precepts.

Further Resources

The following resources may be helpful in keeping pupils safe online:

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

http://www.childnet.com/

http://www.childline.org.uk/

https://www.saferinternet.org.uk/

Person Responsible for reviewing this policy	CE/Head and Primary DSL
Date Ratified by Trustees	09/19
Date of last review	08/18
Date of this review	09/19
Date of next review	09/20