**Dilton Marsh Church of England Primary School**

# **Online Safety and Acceptable use of the Internet Policy**

**Monitoring of this policy:**

This policy has been developed by a working group made up of:

* Head teacher: Jill Hibbs
* Computing/Online-Safety leader: Caroline Tout
* Designated Safeguarding Lead: Sharon Broad

**Schedule for review of this policy:**

|  |  |
| --- | --- |
| The implementation of this policy will be monitored by: | Caroline Tout |
| Monitoring will take place: | Annually |
| The Governing Body will receive a report on the implementation of this policy, generated by the monitoring group: | Annually |
| Next review date: | September 2020 |
| Should serious online safety incidents take place the following should be informed: | Headteacher: Jill Hibbs  Online Safety leader: Caroline Tout  DSL if necessary |

**Impact of this policy:**

The school will monitor the impact of this policy using surveys, logs and questionnaires and adjust the policy accordingly.

**Dilton Marsh Church of England Primary School**

# **Online Safety and Acceptable use of the Internet Policy**

This policy has been written by the school, building on the ‘Wiltshire Learning trust: Online Safety Policy Template 2013’ and government guidance.

This policy should be read in conjunction with other related policies and procedures e.g.

* Safeguarding children and child protection policy
* Child protection procedures and record keeping
* Staff Acceptable Use Policy
* Positive behaviour policy
* Social media policy
* Code of conduct

The internet has become an important aspect of everyday life, to which children need to be able to respond safely and responsibly. At Dilton Marsh Church of England Primary School, we believe that the internet offers a valuable resource for teachers and children, as well as providing new ways to communicate with others worldwide. At the same time there are risks that children may gain access to material that is inappropriate. This policy sets out the measures to be taken that minimises these risks.

**Disclaimer**

Dilton Marsh Church of England Primary School has made every effort to ensure that the information in this policy is accurate and up to date. If errors are brought to our attention we will correct them as soon as is practically possible. However, Dilton Marsh Primary School cannot accept responsibility for any loss, damage or inconvenience caused as a result of reliance on any content in this publication.

**1.The Curriculum**

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to be responsible, competent, confident and creative users of information and communication technology. In delivering the curriculum, teachers plan to integrate the use of communications technology such as web-based resources, e‑mail and mobile learning. Computer skills are vital to access life-long learning and employment. Internet access is an entitlement for students who show a responsible and mature approach to its use. The school has a duty to provide pupils and staff with quality internet access as part of their learning experience.

Benefits of using the internet in education include:

* Access to a variety of worldwide educational resources;
* Inclusion in the National Education Network which connects all UK schools;
* Educational and cultural exchanges between pupils worldwide;
* Vocational, social and leisure use in libraries, clubs and at home;
* Access to experts in many fields for pupils and staff;
* Professional development for staff through access to national developments;
* Educational materials and effective curriculum practice;
* Collaboration across networks of schools, support services and professional associations;
* Improved access to technical support including remote management of networks and automatic system updates;
* Access to learning wherever and whenever convenient.

The school internet access is designed expressly for educational and professional use and includes filtering appropriate to the age of pupils. Pupils learn appropriate internet use and be given clear objectives for internet use. Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils’ age and maturity. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Dilton Marsh Primary School endeavours to ensure that all children are continuously safe and well-informed about online safety. Teachers ensure online safety teaching through a stimulating and appropriate curriculum following the Southwest Grid for Learning curriculum.

**1.1 How will internet access be authorised?**

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. Parental permission is sought. The Acorn Education Trust Academy IT team proactively monitors internet usage for illegal (attempted access of child abuse and incitement for racial hatred) websites and will notify the local police and Wiltshire Council in these instances.

* The school keeps a record of all staff and pupils who are granted internet access.
* New Starter Pack includes the ‘Acceptable Use Policy ‘and guidance for video, sound and images for web publication.
* At Key Stage 1 and 2, access to the internet is by adult demonstration with directly supervised access to specific, approved online materials.
* Parents are informed that pupils will be provided with supervised Internet access.
* Pupils are not issued individual email accounts.

**1.2 Filtering Content:**

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read.

Ideally inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. Pupils are taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

* Pupils are taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.
* Pupils use age-appropriate tools to research Internet content.
* The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
* If staff or pupils discover unsuitable site or content they consider to be inappropriate, the URL (address) and content should be reported to the Academy Trust IT Team.
* No pupils have access to unfiltered content.
* Access for all staff is filtered.
* Website logs are regularly sampled and monitored via the Academy Trust IT Team.
* School ensures that the use of internet derived materials by staff and by pupils complies with copyright law.

#### Pupils are taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.

**1.3 How will the risks be assessed?**

* In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire County Council can accept liability for the material accessed, or any consequences of internet access.
* The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
* Methods to identify, assess and minimise risks are reviewed regularly.
* The Headteacher will ensure that the internet policy is implemented and compliance with the policy monitored.

**2. Managing Content**

Information received via the web, e-mail or text message requires good information-handling skills. In particular, it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read. Pupils need to understand that some content is deliberately misleading, while some is/may be unsuitable from purely a reading-age perspective. Ideally inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed.

* Specific lessons are included within the Computing scheme of work and Digital Citizenship lessons that teaches all pupils how to read for information from web resources.
* Older pupils are taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

**2.1 Website Content:**

* The point of contact on the website is the school address, school e-mail and telephone number. Staff or pupils’ home information will not be published.
* Website photographs that include pupils will be selected carefully.
* Pupils’ full names are not used anywhere on the website, particularly in association with photographs.
* Written permission from parents or carers is obtained before photographs of pupils are published on the school website, school social media pages and local newspapers.
* Class teachers are provided with an updated list of photo permissions and these are kept in classroom at all times.
* Where audio and video are included (e.g. podcasts and video blogging) the nature of the items uploaded will only be included with parental permission.
* Individual class pages (blogs) are only accessible to parents of a child in that class via individual logins.
* The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

**2.2 Managing e-mail:**

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures.

* Pupils may only use approved e-mail accounts on the school system.
* Staff must use official school provided e-mail accounts for all professional communications.
* Pupils must immediately tell a teacher if they receive offensive email.
* Sending images without consent or messages that cause distress and harassment to others are considered significant breaches of school conduct.
* E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

## **3.3 Online Communications and Social Media:**

Online communications, social networking and social media services are filtered in school by their ISP but are likely to be accessible from home.

All staff have been made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They are aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Dilton Marsh Primary School actively encourages pupils about the importance of keeping personal information safe.

* Pupils are taught how to keep personal information safe when using online services. Examples include: real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
* Pupils must not reveal personal details of themselves or others in online communication, or arrange to meet anyone.
* Staff official blogs or wikis should be password protected and run with approval from the SLT.
* Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
* Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private. This is in line with the school’s online safety teaching scheme of work.
* No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.
* Parents wishing to photograph or video at an event should be made aware of the schools expectations and be required to comply with the school’s Acceptable Use Policy (see appendices) as a condition of permission to photograph or record.
* Concerns regarding students’ use of social networking, social media and personal publishing sites will be raised with their parents/carers, particularly when concerning students’ underage use of sites. Any concerns about a pupil’s welfare will be raised with the school’s designated safeguarding lead in accordance with the school’s safeguarding policy.
* Staff personal use of social networking, social media and personal publishing sites (in or out of school) will be discussed as part of staff induction and safe and professional behaviour will be outlined in the Acorn Education Trust ‘Social Media Policy and the Acorn Academy Trust ‘Staff Code of conduct’.
* In line with, ‘Guidance for Safer Working Practice for Adults who Work with Children and Young People’ it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.
* The computing co-ordinator will conduct annual pupil surveys about their home use of ICT. It will gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc.
* The use of online chat is not permitted in school, other than as part of its online learning environment.

**3.4 Mobile phones and personal devices:**

Mobile devices refer to any device that provides access to the internet or internal network for example, tablet (Apple Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras and Smart Watches. Due to the widespread use of personal devices it is essential that schools take steps to ensure mobile devices are used responsibly and that they do not impede teaching and learning.

* Personal mobile devices (including mobile phones, smart watches and tablets) are not to be brought in to school by pupils and the school accepts no responsibility for the loss, theft or damage of such items should they bring in to school.
* In extenuating circumstances, mobile phones may be brought in where parents have specifically requested for use regarding contact arrangements etc. but MUST be handed to the school office at the beginning of the day to be kept securely in the office.
* Staff should not use their mobile device to take photos of students, or text or email students.
* Staff use of mobile devices should follow the points set out in the Acorn Education Trust Code of Conduct.
* School staff, authorised by the Headteacher, may search pupils or their possessions, and confiscate any mobile device which they believe to contravene school policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.
* School staff may confiscate a phone or device if they believe it is being used to contravene the school’s behaviour policy. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
* Where staff may need to contact children, young people and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. e-mail, phone).
* The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community.
* Staff should be provided with school equipment for the taking photos or videos of pupils linked to an educational intention. In exceptional circumstances staff may need to use personal devices for such a purpose and when doing so, should ensure they comply with the Acorn Education Trust Code of Conduct.
* Staff may use their own mobile phones for emergency use on school trips providing they comply with the Acorn Education Trust Code of Conduct.
* Appropriate use of mobile phones will be taught to pupils as part of their PSHE and Digital Citizen programme.
* For the safeguarding of all involved, users are encouraged to connect mobile devices through the school wireless provision and service that allows the ability to filter any device that uses the school internet connection, without having to configure the user’s device.
* Mobile phones will not be used by staff during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of the Senior Leadership Team.

**3.5 Emerging Technologies**

* Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

# **3.6 Cyber Bullying:**

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyber bullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007. DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: <http://www.digizen.org/cyberbullying>

Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school’s behaviour, safeguarding and child protection policies, which will include:

* Clear procedures set out to investigate incidents or allegations of cyber bullying.
* Clear procedures in place to support anyone in the school community affected by cyber bullying.
* All incidents of cyber bullying reported to the school will be recorded.

The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the ISP and the police, if necessary. Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school’s online safety ethos.

* Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.
* There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
* There are clear procedures in place to support anyone in the school community affected by cyberbullying.
* All incidents of cyberbullying reported to the school will be recorded on a behaviour incident log and filled accordingly.
* The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
* Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school’s online safety ethos.

## **3.7 Data Protection**

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 2018 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Schools will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected. For advice and guidance relating to a contravention of the Act, contact Wiltshire council guidance for schools at www.wiltshire.gov.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

## **4. Implementation**

## **4.1 Policy in Practice - Pupils**

Many pupils are very familiar with internet use and the culture that surrounds it. As part of the school’s online safety teaching and awareness-raising it is important to discuss the key features with pupils as appropriate for their age. Pupils may need to be reminded of the school rules at the point of internet use.

All users will be informed that network and internet use will be monitored.

* Pupil instruction regarding responsible and safe use will precede Internet access.
* Online Safety teaching should be integral to the curriculum and raise the awareness and importance of safe and responsible internet use amongst pupils, using the online safety activities from the Southwest Grid for Learning Scheme of work.
* Online Safety teaching will be included in PSHE, Citizenship and/or Computing and cover safe use at school and home.
* Online safety rules and/or copies of the ‘Responsible Internet Rules’ will be visible in the school building.
* Every year the school will have a safer internet week which will highlight the importance of safer internet use through the means of assemblies and teacher-led activities.

## **4.2 Policy in Practice - Parents**

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk.

* Parents’ attention will be drawn to the School Online Safety Policy on the school website.
* A partnership approach with parents will be encouraged. This includes offering parent evenings, regular updates, newsletters, pastoral support and suggestions for safe internet use at home.
* Regular information is provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
* Internet issues will be handled sensitively to inform parents without undue alarm.
* Advice on filtering systems and educational and leisure activities that include acceptable use of the internet are made available to parents.

**4.3 Policy in Practice - Staff**

* All staff including teachers, supply staff, classroom assistants and support staff, will be provided with a copy of this policy.
* All staff must accept the terms of the Acorn Education Trust Code of Conduct before using any internet resource in school which is also applicable to the use of a laptop/tablet provided by the school, for professional purposes.
* Staff should be aware that internet traffic is monitored and reported by the Acorn Academy Trust IT Team and can be traced to the individual user. Discretion and professional conduct is essential.
* Community users of the school’s ICT facilities must sign the acceptable user policy before being granted access.

**4.4 Handling of Complaints**

Parents and teachers must know how and where to report incidents. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the internet use was within or outside school.

* All record of the incident should be kept, e.g. e-mails saved or printed, text messages saved etc. Complaints of a child protection nature must be dealt with in accordance with Child Protection and Safeguarding Policy.
* Any complaint about staff misuse must be referred to the head teacher.
* Pupils and parents will be informed of the complaints procedure.
* Parents and pupils will need to work in partnership with staff to resolve issues.
* There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
* Responsibility for handling incidents will be given to the Headteacher, including any complaint about staff misuse. There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

## **5. Appendices**

1. Responsible Internet Rules for Pupils
2. Responsible Use Agreement Form for staff

# **Responsible Internet Rules:**

**These rules help us to be fair to others and keep everyone safe**.

* I will ask permission before using the internet.
* I will use only my class network login and password.
* I will only open or delete my own files.
* I understand that I must not bring into school my own mobile devices without permission from my teacher.
* Any language (e.g. messages or on multimedia) I use will be polite and sensible.
* I understand that I must never give my home address, phone number or arrange to meet someone.
* I will not access any social media accounts on the school premises.
* If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
* I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
* If I am concerned about my own or my peer’s online safety, I will tell my teacher or a trusted adult at home.

My Name:

My Signature:

My Parent/Carers Name:

My Parent/Carers Signature:

## **Dilton Marsh Church of England Primary School**

**Staff Responsible Use Agreement**

Please complete, sign and return to CT

|  |  |
| --- | --- |
| **Full name:** |  |
| **Role:** |  |

This agreement has been written in line with Dilton Marsh Church of England Primary School Online Safety policy to ensure that all staff are up-to-date with the policies regarding Responsible Internet Use.

Please fill out the following form and hand back to Caroline Tout (Computing and Online Safety Co-Ordinator).

**I confirm:**

* I have read and agree to the terms outlined in the Online Safety and Acceptable Use of the Internet policy,
* I have read and agree to the terms outlined in the Acorn Education Trust Social Media Policy,
* I have read and agree to the terms outlined in the Acorn Education Trust Staff Code of Conduct,
* I have read and agree to the school’s Child Protection Policy.

|  |  |
| --- | --- |
| **Signed:** |  |
| **Date:** |  |