Dunmow St. Mary’s Primary School

Online Safety Policy

September 2016

1. Introduction

The Governing Body of Dunmow St Mary's want all members of our school community to enjoy and benefit from the advantages that technology offers for learning. We do not want the inherent risks associated with access to information, electronic communications and social networking to reduce our use of technology. Instead we want to ensure that our staff, pupils and Governors use the internet in a responsible way so that they do not put themselves or others at risk.

2. Purpose

The purpose of the online safety policy is to:

- Promote the use of technology within the curriculum.
- Protect children from harm.
- Safeguard staff in their contact with pupils and their own use of the internet.
- Ensure that the school fulfils its duty of care to pupils.
- Provide clear expectations for staff and pupils on acceptable use of the internet.

At Dunmow St Mary's we will do this by:

- Providing a **safe internet platform** using Essex County Council's filtered Internet service, which will minimise the chances of pupils encountering unsuitable material.
- Developing a culture of **safe practice** where everyone is aware of the expected standards of online behaviour.
- Teaching our children **to keep themselves and others safe** online and use technology responsibly; this is achieved by working in partnership with parents and carers to raise awareness of the potential risks of internet use.
- Ensuring **online safety is embedded** in the curriculum and actively promoted and a high profile is maintained.
- Ensure all internet users sign an **Acceptable Use Agreement** that sets out their rights and responsibilities and incorporates the school's online safety rules.

3. Roles and Responsibilities

Every member of the school community has a role to play in online safety. Breaches of these roles will be dealt with as laid out in the policy under section 8.

3.1 Headteacher

The Headteacher has ultimate responsibility for online safety issues within the school and staff including:

- The development and implementation and review of the school's online policy
- Ensuring that online safety issues are given a high profile within the school community
- Linking with the Governing Body and parents and carers to promote online safety and report annually to the Governors on the implementation of the school's online safety strategy
- Ensuring online safety is embedded in the curriculum
- Deciding on sanctions against staff and pupils who are in breach of the Acceptable Use Agreement.

3.2 Governing Body

- Members of the Governing Body are subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. In particular Governors should always use business email addresses when conducting school business.
- Monitor the overall effectiveness of the school's online safety policy

3.2.1 Online Safety Officer – Jess Horrocks

The online officer should:

- Ensure that staff and pupils are aware that any online incident should be reported to them. Deal with any low level issues but ensure that the Headteacher is involved with any significant ones.
- Be the first point of contact and advice for school staff, Governors, pupils and parents.
- Keep up to date with online safety issues and advise of new trends, incidents or arising problems, including assessing the impact of emerging technology and the school's response to this.
- Raise the profile of online safety awareness by ensuring access to training and online safety literature.
- Ensure all staff, pupils and Governors have read and signed the Acceptable Use Agreement.
- Liaise with ICT support to ensure that the anti-virus and filtering systems are maintained, audits are carries out and any breaches investigated and records kept.

3.3 School Staff

All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is to:

- Adhere to the school's online policy and acceptable use procedures
- Communicate the schools online policy and acceptable use procedures to pupils
- Keep pupils safe and ensure they receive appropriate supervision and support whilst using the internet.
- Plan use of the internet for lessons and researching online materials and resources
- Report breaches of internet use to the online safety officer (Jess Horrocks).
- Recognise when pupils are at risk from their internet use or have had negative experiences and take appropriate action. Examples of risk might be inappropriate

contact with an adult they have met online; risk from contact with violent extremists; risks from sites advocating suicide, self-harm and anorexia.

- Ensure online safety awareness is embedded in all teaching of the computing curriculum and potentially other parts of the curriculum such as PSHE so that pupils have the opportunity to discuss issues affecting them in an open and safe environment.
- Be able to access pupil's emails and other internet files generated in school and check these periodically to ensure that expectations of behaviour are being met.
- Be aware of those children with special needs or those who may be more vulnerable to risk from internet use (generally those children with a high level of experience and good computer skills coupled with poor social skills)

3.4 Parents and Carers

The school recognises that most children will have internet access at home or on their own mobile devices and might not be as closely supervised as they would be at school. Children may be put at risk in the following ways:

- By being exposed to inappropriate **content** e.g. pornography or information advocating violence ,suicide or illegal behaviour
- By having inappropriate **contact** e.g. through chat rooms, gaming sites, disclosing own personal information or images or cyber bullying.
- By being enticed or persuaded to provide sensitive or private financial information putting themselves or others at risk of unregulated or illegal **commercia**l activity

The school will work with parents and carers to ensure that online safety messages are reinforced at home. We strongly believe that limiting or denying a child access to the internet will not ultimately protect them from the inherent risks. Ultimately we want children to take responsibility for their own choices by understanding the risks and being able to explore online safety issues in the relatively 'safe' environment of school.

3.5 Pupils

- All pupils are expected to read and agree the Acceptable Use Agreement for Pupils annually having discussed it first with their teachers.
- Pupils are taught to take responsibility for their own behaviour and this includes the material they choose to access on the internet and the content of any online communications.
- Pupils are taught that should they encounter an unsuitable site or be unhappy about any online communications they can click on the 'Hector the dolphon' help button which will alert their teacher to any problems.

4. IT and Safe Teaching Practice

School staff and members of the Governing Body should be aware of the importance of maintaining professional standards of behaviour with regard to their own internet use, particularly in relation to their communications with pupils. The following points should be followed to ensure their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

4.1 **Internet and Email Use**

- Access to the school internet system is via individual log-ins and passwords. Without express permission no-one should use other people's passwords or log-ins or obtain access to systems or accounts they are not authorised to use.

- Computers and other devices such as cameras, learnpads, videos etc. belonging to the school are for educational use to assist employees in the performance of their jobs. Only laptops may be taken off the school site without the express prior permission of the Headteacher and these should only be used at home for planning and work related purposes. These devices may also contain sensitive information and should be kept safe and secure at all times.

- School staff are provided with access to electronic media to assist them in fulfilling their roles. Limited or occasional use of electronic media for personal reasons is acceptable as long as does not contravene the rules below which apply to all email communications:

- Emails should not be discriminatory or harassing
- Derogatory to any individual or group
- Obscene, sexually explicit or pornographic
- Defamatory or threatening
- In volition of any license governing the use of software or copy write

- The school reserves the right to monitor electronic media and communications for cost analysis, resource allocation and detecting patterns of use that indicate employees are violating school policies or engaging in illegal activities. Employees should not assume electronic communications are completely private.

- Under no circumstances should pupil-named data be transmitted over the internet or email. The office has use of encrypted data systems for this purpose.

- No unauthorised downloading of software is allowed. Only software registered through the school may be downloaded. As the school uses a shared server any viruses arising from such actin have the potential to harm/destroy more than a single computer.

4.2 Photographs/ Video/ Images

- Photographic and video images of pupils should only be taken by staff in connection with educational purposes.

- Staff should use school equipment and only store images on the school network. On occasion, staff may use personal cameras, phones or iPads to take photographs. Please note that these should be immediately uploaded to the school network and must not be taken off site or stored on personal devices.

- The school has written permission for pupils photographs to be used on the school website and/or for marketing purposes. The school office has a list of exceptions (children who do not have written permission). Names should never be used in conjunction with photographs and group photographs are better than individual ones.

Any images or articles to be published externally should be agreed with the School Business Manager beforehand.

4.3 Social Networking

- Staff and Governors should take care regarding the content of and access to their own social networking sites. Any information that they publish or share may be accessible to the public at large.

- Staff and Governors should not discuss individuals – pupils, staff, parents, or Governors on social networking sites. To do so would constitute a serious breach of confidentiality and data protection procedures.

- Staff and Governors should not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context. Neither should they use email or phones to contact pupil outside school hours.

- Contact between staff and parents and pupils on school business should be done using school equipment and email addresses. Numbers should not be stored on personal phones

- Staff should not accept friend requests from pupils or past pupils.

5. Using the Internet in the Classroom

- Teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.

- Pupils should not be allowed to aimlessly 'surf' the internet and all use should have a clearly defined educational purpose.

- When using the internet children should receive an appropriate level of supervision for their age and understanding.

- The school Email system DB Primary allows pupils to send emails to others within the school.

- Social Networking Sites such as Facebook, Twitter and MySpace allow users to publish information that can be seen by anyone and as such are not suitable for use within a school.

- Newsgroups and forums are sites that enable users to discuss ideas and share ideas online. Teachers may feel these have an educational value and may use these if appropriate and monitored carefully.

- Chat rooms and Instant Messaging and Gaming Sites are not hosted by the school system and not appropriate for use in school.

- If a teacher or pupil unintentionally opens a website with content that is upsetting or inappropriate they should immediately close the screen. Teachers should reassure the pupil they have done nothing wrong and reinforce the online safety message. The incident should be reported to the Online Safety Officer and the URL and website provided so that the site can be blocked for the future.

6. Teaching Online Safety

Pupils are taught all elements of online safety included in the computing curriculum including but not limited to:

- Keeping personal information private e.g. not to give out personal details to anyone online that may help to identify or locate them or anyone else for example home address, name of school or clubs identified.
- Only using moderated chat rooms that require registration and are specifically for their age group.
- Not uploading personal photos of themselves or others onto sites and to take care regarding what information is posted online as there is no control of who sees images.
- Setting up security and privacy settings on sites.
- Behaving responsibly whilst online and keep communications polite.
- Not responding to any hurtful or distressful messages but to let their parents, carers or teachers know so action can be taken.
- Not arranging to meet anyone whom they have only met online or go offline with anyone they meet in a chat room.
- identifying where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In this way they can become responsible, confident, competent and creative users of information and communication technology.

7. Potential Abuse of Internet

7.1 Intentional access of inappropriate websites by a pupil

If a pupil deliberately accesses inappropriate or banned websites they will be in breach of the Acceptable Use Agreement. The incident should be reported to the Online Safety Officer and the Headteacher who will decide an appropriate course of action.

7.2 Inappropriate use of IT by staff or Governors

If a member of staff witnesses misuse of IT by a colleague they should report this immediately to the Headteacher or Chair of Governors. This school's disciplinary procedure will be invoked and followed.

7.3 Cyber bulling

Cyberbullying is defined as the use of technology such as email, messaging and social networking sites to deliberately hurt, upset, harass or threaten someone. The internet allows this form of bullying to continue past school hours and invades the victim's home and personal life. It can affect pupils and staff members.

Bullying may take the form of:

- rude, abusive or threatening messages via email or text
- posting insulting, derogatory or defamatory statements on blogs or social networking sites
- Setting up web sites that specifically target the victim
- Making or sharing derogatory or embarrassing images or videos of someone via mobile phones or email (for example, sexting/"happy slapping").

In extreme cases cyber bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

The school's behaviour policy covers the issue of cyber bullying, however, the key points to note are as follows:

1. Any incidents of cyber bullying should be reported to the Online Safety Officer or Headteacher. These will be dealt with in line with our behaviour policy.
2. Extreme incidents will be reported to the Police.
3. Pupils will be taught
   - To only give out mobile phone numbers and email addresses to people they trust
   - To only allow close friends whom they trust to have access to their social networking page. Please note that most social networking sites have a minimum age of 13 and as such children and parents will be advised not to have these for primary age children.
   - Not to send or post inappropriate images of themselves
   - Not to respond to offensive, upsetting or hurtful messages
   - To report any problems or worries to their parents and teacher immediately.

7.4 Cyber bulling of employees

It is entirely possible that employees at the school may themselves become victims of cyberbullying either by pupils or parents. Further details and advice for employees is available in our 'Safety and Respect' policy.

8. Sanctions for misuse of school ICT

Pupils who break the terms of their Acceptable Use Agreement will be dealt with under the terms of the school's behaviour policy.
Staff who misuse ICT will be dealt with under the school's Disciplinary Procedures.

Pupil Acceptable Use Agreement:

Dunmow St. Mary's Primary School

Name: ______________________________ Class: _____________________

Responsible Internet and Computer Use Agreement

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will:

1. Use the school computers, Internet and all our technological equipment sensibly and carefully.
2. Only use my own username and password to access the computer network.
3. Ask permission before entering any website, unless my teacher has already approved that site.
4. Not enter chat rooms or leave messages on bulletin boards or tell people about myself online. (I will not tell them my name, anything about where I live or where I go to school or upload any photos.)
5. Tell a teacher immediately if I see anything I am unhappy with or I receive messages I do not like.
6. Not respond to any nasty message that makes me feel upset or uncomfortable.
7. Never insert my personal details, home address, or telephone numbers on the Internet or in an e-mail.
8. Only e-mail people or open e-mails from people I know, or my teacher has approved.
9. Always be polite and kind and use appropriate language when sending e-mails.
10. Not look at or delete other people's files without their permission.

I understand that if I deliberately break these rules, I could be stopped from using the school network and accessing the Internet.

Signed: ___________________________ Date: _________________-

Employee Acceptable Use Agreement

(To be signed and a copy stored on file)

I have read and understood the Online Safety Policy. I agree to abide by the rules and conditions that are laid out in it. I understand that I have no expectations of privacy when I use any of the telecommunication equipment or services provided by school. I am aware that violations of this guideline on appropriate use of the e-mail, Internet systems and participation in social networking sites may subject me to disciplinary action, including termination from employment, legal action and criminal liability. I further understand that my use of e-mail, Internet systems and participation in social networking sites may reflect on the image of Dunmow St Mary's Primary School to our pupils, parents, Governors and suppliers and that I have responsibility to maintain a positive representation of the school.

Dated: _________________

____ Signature of employee

____ Printed name of employee