# E- Safety & Use of Internet Policy

# Debden CE Primary Academy

Reviewed by: Louise Gurney June 2016
Shared with staff: June 2016
Shared with Governors: July 2016
Review date: July 2018

**Debden Church of England Primary Academy**

**Use of the Internet (by pupils and staff) policy**

**Introduction**
Internet use is part of the statutory curriculum and is a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security**.**
Usually the resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated information, at times they will be able to move beyond these to sites unfamiliar to the teacher.

The problems and issues that have been highlighted by the media concern all schools. Whilst some of the media interest is hype, there is genuine cause for concern that children might access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Debden with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Establish the ground rules we have in school for using the Internet
- Ensure pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Ensure pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Ensure pupils will use age-appropriate tools to research Internet content.
- Ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence. 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 carers.

- Promote an awareness and commitment to online safety throughout the school community
- Ensure that online safety education is embedded within the curriculum
- Offer guidance to staff about the use of social networking sites.

At Debden Church of England Primary, 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.

**Security**
The school has obtained LA guidance on Internet security and following their suggestion has based its policy on the DfES site http://safety.ngfl.gov.uk/schools/

**Using the Internet to enhance education**
The benefits include:

- Access to a wide variety of educational resources including libraries, art galleries and museums;
- Rapid and cost-effective world-wide communication;
- Gaining an understanding of people and cultures around the globe;
- Staff professional development through access to new curriculum materials, expert knowledge and practice;
- Exchange of curriculum and administrative data with the Local Authority and DCSF;
- Social and leisure use;
- Greatly increased skills in Literacy, particularly in being able to research, read and appraise critically and them communicate what is important to others;
- The school intends to teach pupils about the vast information resources available on the Internet, using it as a planned part of many lessons;
- All staff will review and evaluate resources available on web sites appropriate tot the age range and ability of the pupils being taught.

**Pupils' Access to the Internet**
Debden Primary School will use the Essex County Council's filtered Internet service, which will minimize the chances of pupils encountering unsuitable material. Debden will normally only allow children to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed towards every computer screen. Members of staff will be aware of the potential for misuse and will be responsible for explaining expectations of proper use to pupils.

Teachers will have access to pupils' emails and other Internet files generated in school, and will check these periodically to ensure that expectations of behaviour are being met.

**Expectation of pupils using the Internet**

- At Debden we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use.
- Pupils using the World Wide Web are expected not deliberately to seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider can block further access to the site.
- Pupils are expected not to use any rude or offensive language in their email communications, and contact only people they know or those the teacher has approved. They will be taught the rules of etiquette for email and will be expected to follow them.
- Pupils must ask permission before accessing the Internet and have a clear idea of why they are using it.
- Pupils must not access other people's files unless they have permission to do so.
- Computers and school laptops should only be used for school work and homework unless permission has been given otherwise.
- No program files may be downloaded from the Internet to the computer, to prevent corruption of data and to avoid viruses
- No programs on CD Rom or flash drive/memory sticks should be brought in from home for use in school. This is for both legal and security reasons. Homework completed at home may be brought in on a memory stick, but will be virus scanned by the class teacher before use.
- No personal information such as phone numbers and addresses should be given out and no arrangements should be made to meet someone via the Internet/email, unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and may be denied access to Internet resources. They will also be subject to the general disciplinary procedures of the school.
- Pupils should understand the importance of reporting abuse, misuse or access to inappropriate materials
- Pupils should understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school
- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.
- All pupils must read (with the help of parents), understand, sign and adhere to the ICT Pupil Acceptable Use agreement annually

**Expectation of Parents/carers**:

- To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren
- To consult with the school if they have any concerns about their children's use of technology
- To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images

**Appendix 2 - Employee Agreement for the use of school technology:**

**Purpose**

- To remain competitive, better serve our pupils and provide our employees with the best tools to do their jobs in Debden Primary School for and on behalf of Essex County Council (hereinafter called 'the school') makes available to our workforce access to one or more forms of electronic media and services, including computers, e-mail, telephones, voicemail, fax machines, external electronic bulletin boards, wire services, online services, intranet, Internet and the World Wide Web.

- The school encourages the use of these media and associated services because they can make communication more efficient and effective and because they are valuable sources of information about educational issues, ideas, technology, and new products and services. However, all employees and everyone connected with the organisation should remember that electronic media and services provided by the school are school property and their purpose is to facilitate and support school business. All computer users have the responsibility to use these resources in a professional, ethical, and lawful manner.

- To ensure that all employees are responsible, the following guidelines have been established for using e-mail and the Internet. No policy can lay down rules to cover every possible situation. Instead, it is designed to express the philosophy of the school and set forth general principles when using electronic media and services.

- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.

- The school does not allow pupils the use of mobile phones. Staff are not allowed to use mobile phones in lesson time and when they are on duty; at other times they can, if necessary, use them.

**Prohibited communications**

Electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is:

1. Discriminatory or harassing;
2. Derogatory to any individual or group;
3. Obscene, sexually explicit or pornographic;
4. Defamatory or threatening;
5. In violation of any license governing the use of software; or
6. Engaged in for any purpose that is illegal or contrary to the school's policy or interests.

**Personal use**

The computers, electronic media and services provided by the school are primarily for educational use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their educational purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

**Access to employee communications**

The school reserves the right to routinely gather logs for most electronic activities or monitor employee communications directly, e.g., telephone numbers dialed, sites

accessed, call length, and time at which calls are made, for the following purposes:
1. Cost analysis;
2. Resource allocation;
3. Optimum technical management of information resources; and
4. Detecting patterns of use that indicate employees are violating school policies or engaging in illegal activity.

The school reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other school policies.

Employees should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit, they should use other means.

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

**Software**
To prevent computer viruses from being transmitted through the school's computer system, unauthorized downloading of any unauthorized software is strictly prohibited. Only software registered through the school may be downloaded. Employees should use virus trapping software on any home computer that is used to download planning or other information onto the school computers. Employees should contact the headteacher if they have any questions.

**Security/appropriate use**
Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by school management, employees are prohibited from engaging in, or attempting to engage in:
1. Hacking or obtaining access to systems or accounts they are not authorized to use.
2. Using other people's log-ins or passwords.
3. Breaching, testing, or monitoring computer or network security measures.

No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

Anyone obtaining electronic assess to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

**Encryption**
Employees can use encryption software supplied to them by the systems administrator for purposes of safeguarding sensitive or confidential business information. Employees who use encryption on files stored on a school computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files.

**Participation in online forums**

Employees should remember that any messages or information sent on school-provided facilities to one or more individuals via an electronic network - for example, Internet mailing lists, bulletin boards, and online services - are statements identifiable and attributable to the school.

The school recognises that participation in some forums might be important to the performance of an employee's job. For instance, an employee might find the answer to a technical problem by consulting members of a news group devoted to the technical area.

**Violations**
Any employee who abuses the privilege of their access to e-mail or the Internet in violation of this policy will be subject to corrective action, including possible disciplinary action, legal action, and criminal liability.

**Advice to staff on the use of social networking sites**
- There have been many issues with Facebook and other social networking sites in schools over the last couple of years.
- The internet is a public domain not a private one and staff in schools must be aware that information which they share and post is accessible to the public at large.
- It is therefore particularly important that staff do not name or 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.
- All staff in schools must also be aware that they are particularly vulnerable to accusations of inappropriate behaviour, even outside of school, and that these could potentially give rise to the involvement of the GTC and formal disciplinary procedures.
- All school staff, particularly teachers, risk exposure in the press and potential complaints to headteachers, governors and the Local Authority when information posted on the Internet suggests behaviour which compromises their position as role models to pupils..
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.

**Our school offers the following advice to staff/volunteers**
1. Ensure that you do not post any photographs on the Internet which could give cause for embarrassment.
2. Do not post any comments which could compromise your own integrity or which could bring the school, your colleagues, parents or the school community into disrepute.
3. Do not discuss school matters, including comments about pupils, staff, parents or governor on social networking sites.
4. Check that you are happy with the privacy levels on your pages and review these settings regularly.
5. You are very strongly advised **not to allow pupils to become 'friends'** on these sites. This is because it is deemed to be inappropriate to encourage out-of-school relationships with pupils and because of the nature of some of the likely content of material on sites used by adults.
6. If a complaint is received about a member of school staff then this will be dealt with under the school's disciplinary procedures and in consultation with Essex County Council's HR Schools' Team.
7. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

8. All staff must read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction.
9. At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

**Communication:**

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

**Handling Incidents:**

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

**Review and Monitoring**

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

**Staff and governor training**

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

**Parent awareness and training**

- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.
- Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.