Melton Primary School

Online Safety and Acceptable Use of ICT Policy

Written by:	Sandy Thornton
Reviewed by:	Premises and Child Welfare Committee
Signed by:	Katharina Thomas / Tessa Amos/Mike Burges/ Mark Girling
Approved date:	Summer 2017
Review due:	Summer 2018 (ideally alongside Safeguarding policy)

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

This policy must be read in conjunction with the following policies and guidance:

- Safeguarding Policy
- Use of Restraint in School Policy
- Whistle Blowing Policy
- Staff Information Booklet
- Equality Policy
- ICT Policy

1. Introduction

Technology has had a massive impact on our day to day lives. The internet is now regarded as an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. For the purposes of this policy it is important to clarify what is included under the umbrella term of 'technology'. Within school technology is defined as being that which delivers information or allows us to communicate with the wider community. This includes desktop PCs, laptops/notebooks, slate technology, mobile phones and the internet referencing many developing mobile technologies. Technological skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

Dr Tanya Byron, in her landmark report 'Safer Children in a Digital World', published in March 2008, set out a challenging agenda for Government, its partners, industry and the third sector, to work together to make children safer when using the internet and video games. The Government of the time accepted all of Dr Byron's recommendations in full, signifying our commitment to children's safety when using new technology. To meet this commitment, we will work with children, parents and staff, and build on the consultative and collaborative approach.

The internet is no longer restricted to a computer, but can accessed on an increasing number of devices. Therefore this document does not set out to restrict access to technologies and online content, but rather sets out guidelines which 'empower learners to develop safe and responsible online behaviours to protect themselves' (Becta; AUPs in Context: establishing safe and responsible behaviours. 2009). Also referring to the National Curriculum Document 2014 which states, " [children in Key Stage Two should] use search engines effectively and appreciate how results are selected and ranked; be discerning in their evaluation of digital content; respect individuals and intellectual property; use technology responsibly, securely, and safely; recognise the impacts of technology on their and others' lives, and how they change over time".

This policy sets out an ethos for an E-Sense curriculum which will help children protect themselves in the wider world.

2. Aims for this policy

This policy sets out the guidance for all stakeholders on appropriate and acceptable use of ICT, the internet, and subsequently the school's website and online profile. When using the term 'Stakeholders' the policy is referring to all parties with whom the responsibility of appropriate usage lies i.e. the School's Governing Body, all School staff, pupils and parents/carers.

This policy will set out guidelines on the following:

- Acceptable use of technology within school for all stakeholders; their rights and responsibilities.
- The effect of the internet on learning and teaching within the school.
- Core principles of internet safety including parent involvement to underpin 'whole school community' approach to online safety
- The appropriate use of the School's Learning Platform.
- Dealing with and recording misuse inside and outside school
- Online Safety and the curriculum, which is termed at Melton the 'e-sense' curriculum

This policy also works in conjunction with the ICT Policy.

3. Acceptable Use of Technology within school

School Responsibilities

3.1 The Governing Body is responsible for ensuring that its employees act in a lawful manner, making appropriate use of school technologies for approved purposes only.

3.2 The Governing Body is responsible for adopting relevant policies and the Headteacher/Curriculum Leader are responsible for ensuring that staff are aware of their contents.

3.3 If the Headteacher has reason to believe that any ICT equipment has been misused, he/she should consult the Area Personnel Officer or Education Lead Officer at the Area Office for advice without delay. The Area Personnel Officer will agree with the Headteacher and CSD's Policy and Compliance Manager an appropriate strategy for the investigation of the allegations. Incidents will be investigated in a timely manner in accordance with agreed procedures.

3.4 Headteachers should make it clear that internal school staff should not carry out any investigations unless they are both qualified and authorised to do so.

3.5 Headteachers should ensure that opportunities are provided for training and the sharing of information between stakeholders.

User Responsibilities

3.6 Staff found to be in breach of this policy may be disciplined in accordance with the disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in termination of employment. Users must report all suspected breaches of this policy to the Headteacher which will subsequently be investigated and be recorded as an E-Sense incident.

3.7 Staff will be given a succinct version of this document to be signed and referenced to at the beginning of each academic year. This document will be countersigned by the Headteacher and kept in the user's personnel file.

3.8 Users and their managers are responsible for ensuring that adequate induction, training and support is undertaken to implement this policy. At least one member of teaching staff will be accredited by CEOP or a similar agency.

3.9 All users are expected to act in a responsible, ethical and lawful manner with the understanding that school electronic and manual information may be accessible to the public under the Freedom of Information Act 2000. Users should uphold privacy and confidentiality in accordance with the Data Protection Act 1998. Care must also be taken not to breach another person's copyright, trademark or design, not to publish any defamatory content.

3.10 No one may use ICT resources in violation of license agreements, copyright, contracts or national laws, or the Standing Orders, policies, rules or regulations of the school or the County Council.

3.11 Users are required to protect their password and not share their account details with others for their use, nor utilise another users' account or misrepresent their identity for any reason. Users must not under any circumstances reveal their password to anyone else.

3.12 No user shall access (e.g., read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or the law.

3.13 Users must not load or download software on any device without the authorisation of the Headteacher. Periodic audits of software held on ICT equipment will be undertaken.

3.14 Users must take care to store sensitive information, e.g. pupil data should be encrypted and its password protected, on all school systems, including laptops.

3.15 Network connected devices must have school approved anti-virus software installed and activated. Users may not turn off anti-virus software. All users of ICT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive program on any ICT resource.

3.16 No one may knowingly or willingly interfere with the security mechanisms or integrity of ICT resources. No one may use ICT resources to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks. Access to networks will be monitored.

3.17 Within the terms of the Data Protection Act 1998, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the County Council or school may record or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:

- There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy.
- An account appears to be engaged in unusual or unusually excessive activity.
- It is necessary to do so to protect the integrity, security, or functionality of ICT resources or to protect the County Council or its partners from liability.
- Establishing the existence of facts relevant to the business.
- Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of ICT facilities.
- Ensuring effective operation of ICT facilities.
- Determining if communications are relevant to the business (e.g. in the last resort where an employee is off sick or on holiday and business continuity is threatened).
- It is otherwise permitted or required by law.

3.18 Do not send private, sensitive or confidential information by unencrypted email – particularly to an external recipient – if accidental disclosure could lead to significant harm or embarrassment. Anonymise personal data where possible e.g. by using initials. Use passwords on sensitive documents that must be sent to external recipients.

3.19 Websites should not be created on school equipment without the written permission of the Headteacher.

3.20 No one may use ICT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a school account.

3.21 The following content should not be created or accessed on ICT equipment at any time:

- Pornography and “top-shelf” adult content
- Material that gratuitously displays images of violence, injury or death
- Material that is likely to lead to the harassment of others
- Material that promotes intolerance and discrimination on grounds of race, sex, disability, sexual orientation, religion or age
- Material relating to criminal activity, e.g. buying and selling illegal drugs
- Material relating to any other unlawful activity e.g. breach of copyright
- Material that may generate security risks and encourage computer misuse

3.22 It is possible to access or be directed to unacceptable Internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If staff have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Headteacher. This may avoid problems later should monitoring systems be alerted to the content.

4. Personal Use and Privacy.

In the course of normal operations, ICT resources are to be used for business purposes only. The school permits limited personal use of ICT facilities by authorised users subject to the following limitations:

- Personal use must be in the user’s own time and must not impact upon work efficiency or costs.
- The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided.
- Personal use must not be of a commercial or profit-making nature.
- Personal use must not be of a nature that competes with the business of the school or conflicts with an employee’s obligations.

In June, July, September 2013 both Staff and Pupils were consulted separately about E-Sense around our school community and what they feel is acceptable. It was a consensus view that social networking sites and purchasing sites are inappropriate for school use and therefore should be restricted, or ‘filtered’.

5. MOBILE PHONE COMMUNICATION AND INSTANT MESSAGING

5.1 Staff mobile phones should be securely located away from children during teaching periods.

5.2 Staff are advised not to give their home telephone number or their mobile phone number to pupils or parents. Mobile phone communication should be used sparingly and only when deemed necessary.

5.3 Photographs and videos of pupils should not be taken with mobile phones.

5.4 Staff are advised not to make use of pupils’ mobile phone numbers either to make or receive phone calls or to send to or receive from pupils text messages other than for approved school business.

5.5 Staff should only communicate electronically with pupils from school accounts on approved school business, e.g. coursework through the learning platform

5.6 Staff should not enter into instant messaging communications with pupils unless this is for the purpose of educational purposes and in the context to the eCadet programme and monitored.

6. Learning and Teaching using the Internet within the School

The Internet is an essential element in 21st century 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. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Significant educational benefits should result from curriculum internet use including access to information from around the world and the ability to communicate widely and to publish easily. Curriculum internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful internet use will also reduce the opportunities for activities of dubious worth.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils and currently managed by the school.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use from an early stage (most probably Year One).
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity. It is the class teacher's responsibility to check the appropriateness of the internet links that he/she may use in class.
- All users of the internet in school will be aware of Copyright and will not knowingly use another's content as their own without due acknowledgement.
- A dedicated E-Sense curriculum is taught from Reception up to Year 6.
- Children will be aware of reporting procedures if they see or experience something which makes them feel uncomfortable.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

7. Core Principles of Online Safety.

The internet is becoming as commonplace as the telephone or television and its effective use is an essential life-skill. Unmediated internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. This policy helps to ensure responsible usage and the safety of pupils. Online safety rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

The school owns the computer network and can set rules for its use. For good internet safety to work all stakeholders need to be involved and informed of the decisions made. Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. Parental permission should be sought on starting at the school (at whatever stage).

7.1 Responsibility

Online safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of internet and other communication technologies. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully. There are a number of technical solutions to help limit internet access appropriately, although it is the appropriateness and consistency of the school's e-sense policy that is of overriding importance. Primary responsibility lies with the school's governing body and the head teacher. However all staff should be aware of their roles and responsibilities when using the internet within school for use both with classes and for their own professional use.

7.2 Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign this policy before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents/children will be asked to sign and return a consent form for pupil access.
- It is the school's responsibility to ensure that good use of filters is in place and that LAN settings are secure. The School's Broadband use is filtered by systems provided by the school.
- Pupils are educated to be responsible online citizens.

8. Appropriate Use of the School Website.

The school's website is a maintained and monitored extension of the school environment. It is the Head teacher's responsibility as overall 'Super User' to govern appropriate use of the site. Alongside the Head teacher, other 'Super Users' should also monitor appropriate use on a regular basis.

8.1 Published content and the school's website

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate through 'spot-checks'.

8.2 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully for use on school website. Reporting and Assessment systems, where information is 'Cloud based' is password protect.
- Pupils full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents/carers.

8.3 Pupils roles and responsibilities

- All children will be educated through the dedicated 'E-Sense' curriculum on the following points:
  - Not to share passwords with others, except than with their parent/carer.
  - Children to have responsibility for their own online behaviour, any posts or blogs that are deemed to be inappropriate by the 'Super Users' will result in the user being suspended from using the school network for a stipulated duration.

9. Dealing with Misuse

Misuse is defined as any action by a stakeholder that is deemed to be inappropriate or has a negative inflection on the school and/or children. This may include:

- Inappropriate use of language through the website or indeed any other internet sites such as social networking sites, directed towards another user.
- The inclusion of personal information without consultation with Head Teacher that could result in a detrimental effect on a child/member of staff/school.

- The use of material that may generate security risks and encourage computer/internet misuse.
- Links made to internet sites that promote criminal activity, intolerance and discrimination.
- Links made to internet sites that gratuitously display images of violence, injury or death.

Staff found to be in breach of this policy may be disciplined in accordance with the disciplinary procedure. In certain circumstances, breach of this policy may be considered as gross misconduct resulting in termination of employment. Users must report all suspected breaches of this policy (or indeed breaches of any policy relating to acceptable use of ICT in school), to the Head Teacher who will take appropriate action. This will include all suspected incidents of misuse to be discussed with the Chair of Governors, Online Safety-Governor, Headteacher and Online Safety Co-ordinator. This would the feed back to the whole of the Governing body.

Children who are suspected to be in breach of this policy will have their internet use monitored. If an incident is confirmed, the user will be suspended pending a full investigation. Parents/carers will be informed and discussions relating to further use will take part. These will involve a representative of the governing body, Head Teacher, a named 'Super User' and parents/carers. The child will be involved as appropriate. Any online safety issues which may arise will be recorded in the Online Safety log which is kept in the Headteacher's office. The number of incidents are reported to the Governing Body.
Misuse is a serious issue and will be dealt with efficiently and appropriately.

Signed...(Head Teacher)

Signed...(_Online Safety Co-ordinator)

Signed...(Chair of Governors)

Signed…………………………………………..(Online Safety Governor/Named Safeguarding Governor)

Date: ....