E-Safety & ICT Acceptable Use Policy

June 2019

Rationale

As a primary school working with our local, national and international communities, ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At MY Schools Together, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the ICT Acceptable Use Agreements (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, and portable media players, etc).

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school the Governing Body has ultimate responsibility to ensure that the policy and practices are embedded and monitored. This responsibility is delegated to the Head. Any extra permission given by the Head must be recorded (e.g. memos, minutes from meetings) in order to be valid.

The named person (Safeguarding Officer) SLT have the responsibility of ensuring this policy is upheld by all members of the school community and that they have been made aware of the implication this has. It is the role of these members of staff to keep abreast of current issues and guidance through organisations such as the LA, Becta, CEOP (Child Exploitation and Online Protection), Childnet and Local Authority Safeguarding Children Board.

This policy, supported by the school's ICT Acceptable Use Agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is

linked to the following mandatory school policies: child protection, health and safety, RSE Policy, safeguarding policy and behaviour/pupil discipline (including the anti-bullying) policy. E-safety skills development for staff

- Our staff receive regular information and training on e-safety issues in the form of full staff meetings and memos via First Class.
- New staff receive information on the school's ICT Acceptable Use Policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

Communicating the school e-safety messages

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be regularly monitored.
- E-safety posters will be prominently displayed, especially in the ICT suite.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety. We regularly monitor and assess our pupils' understanding of e-safety.

- The school provides opportunities within a range of curriculum areas and discrete Computing lessons to teach about e-safety (in accordance with the medium term planning.)
- Educating pupils on the dangers of technologies that maybe encountered outside school may also be done informally when opportunities arise.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff have access to this through SIMS and CPOMS for all pupil sensitive data. Staff and pupils are regularly reminded of the need for password security.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. Level of access is determined by the Executive Headteacher. Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any school/pupil data.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

- All staff must read and agree to the 'ICT Acceptable Use Agreement' before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- School internet access is controlled through the LA's web filtering service.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the class teacher who must inform an e-safety co-ordinator.
- It is the responsibility of the school, by delegation to the technical support; to ensure that Anti-virus protection (Sophos) is installed and kept up-to-date on all school machines.
- If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT Technician.
- If there are any issues related to viruses or anti-virus software, the ICT Technician should be informed through the 'ICT Jobs' conference on First Class.

Managing other Web 2 technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school denies access to social networking sites such as Facebook to pupils within school.
- Staff remind pupils that social media sites should not be accessed till the illegal age of 13. Parents are reminded of this.
- There should be no communication between staff and pupils through social networking sites such as Facebook, Linked-in and Twitter (or similar - this list is not exhaustive)
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, details, IM/emailaddress,specifichobbies/interests) Our pupils are advised to set and maintain

profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.

.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil using their personal device.
- Staff may take pictures of pupils on trips or curriculum related experiences. They must upload these images to the schools' network as soon as possible and delete the image from their personal device. If possible we prefer staff to take such images on the schools' devices (ie iPads). Curriculum related visitors may take photographs of the session they are delivering under the supervision of the organising teacher. Teachers must ask how the images will be used. If unsure whether the purpose meets the requirements of this policy they must refer the matter to the Business Manager.
- Parents may take photographs/videos of concerts, assemblies on their mobile devices but they must be reminded not to share the images on social media.
- Pupils are not allowed to bring personal mobile devices/phones to school unless authorised by the Executive Headteacher & Head of School.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or internationally.

- The school gives all staff their own email (First Class) account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal

details about themselves or others in e-mail communication, or arranging to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the SLT or Business Manager if they receive an offensive e-mail.
- Pupils are introduced to email as part of the Computing Curriculum

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils.
- Pupils are not permitted to use personal digital equipment, including mobile phones, cameras or tablets to record images of others, this includes when on school trips. With the consent of the class teacher, pupils are permitted to take digital cameras from school to record images and can download these images on the school network.
- Staff **must not** take images of a child's injuries or bruising even if we are requested to do so by Social Care or Health & Safety Team.

Publishing pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time.

Pupils' full names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Before posting pupils' work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

Images/ films of children are stored on the school's network.

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Executive Headteacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.
- Teaching Staff have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

Misuse and Infringements

Staff are aware that breaching the conditions within this policy may result in disciplinary action, suspension or dismissal depending upon the seriousness of the offence and following investigation by the Executive Headteacher.

Complaints

- Complaints relating to e-safety should be made to the Executive Headteacher.
- All incidents will be logged and followed up.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and must be reported to the Named person (Safeguarding Officer).
- Pupils and parents will be informed of the complaints procedure.

Inappropriate material (see ICT Acceptable Use Policy Appendix 1 and 2)

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety co-ordinators.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Business Manager, depending on the seriousness of the offence; investigation by the Executive Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers are asked to read through and sign ICT acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to e-safety where appropriate in the form of;
    - Information sessions
    - Posters
    - Learning Platform postings/links to further information
    - Newsletter items
- Parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Parents/carers are expected to reinforce the guidance from school when using technologies at home. The school will not be responsible for communications between pupils' outside school through social networking sites.

ICT Acceptable Use Agreement (AUA)

POLICY STATEMENT

The Governing Body recognises the use of ICT as an important resource for teaching, learning and personal development. It actively encourages staff to take full advantage of the potential for ICT to enhance development in all areas of the curriculum and school administration. It is also recognised by the Governing Body that along with these benefits there are also responsibilities, especially for ensuring that children are protected from contact with inappropriate materials.

In addition to their normal access to the school's ICT systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of ICT equipment and e-mail and internet facilities during their own time subject to such use:

1. *not depriving pupils of the use of the equipment*
   and/or
2. *not interfering with the proper performance of the staff member's duties*

Whilst the school's ICT systems may be used for both work-related and for personal reasons the Governing Body expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the Governing Body at all times and must never compromise the high standards of Safeguarding expected by all members of the staff.

The use of computer equipment, including laptop computers and iPads that are on loan to staff by the school for their personal use at home is covered under this policy. Staff who have equipment on loan are responsible for its safekeeping and for ensuring that it is used in compliance with this policy.

GUIDANCE ON THE USE OF SCHOOL ICT FACILITIES

Whilst it is not possible to cover all eventualities, the following information is published as guidance for staff on the expectations of the Governing Body. Any non-conformance to this policy or operation outside statutory legal compliance may be grounds for disciplinary action being taken up to and including disciplinary action

Further guidance on the responsible use of ICT facilities are contained in the Council document *"Internet Access Policy for Schools"*.

E-mail and Internet usage

The following uses of the school's ICT system are prohibited and may in certain circumstances amount to gross misconduct and could result in dismissal:

1. *to gain access to, and/or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it*

2. *to gain access to, and/or for the publication and distribution of material promoting racial hatred*

3. *for the purpose of bullying or harassment, or for or in connection with discrimination or denigration on the grounds of gender, race, disability or sexual orientation*

4. *for the publication and/or distribution of libellous statements or material which defames or degrades others*

5. *for the publication and distribution of personal data without either consent or justification*
6. *where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination*
7. *to participate in on-line gambling*
8. *where the use infringes copyright law*
9. *to gain unauthorised access to internal or external computer systems (commonly known as hacking)*
10. *to enable or assist others to breach the Governors' expectations as set out in this policy*

Additionally, the following uses of school ICT facilities are not permitted and could lead to disciplinary action being taken:

1. *for participation in "chain" e-mail correspondence*
2. *in pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade union representatives)*
3. *to access ICT facilities using another person's password, or to post anonymous messages or forge e-mail messages using another person's identity.*

Use of School ICT Equipment

Users of school ICT equipment:

1. *must not share and must treat as confidential any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries*
2. *must report any known breach of password confidentiality to the Executive Headteacher or Business Manager as soon as possible*
3. *must report known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's ICT systems*
4. *must not install software on the school's ICT systems, including freeware and shareware*
5. *must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures*

Legal Framework:

Staff are made aware, through this policy ,that laws relating to libel, defamation, harassment and copyright law may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice Act and Public order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003
- Copyright, Designs and Patents Act 1988
- Human Rights Act 1998
- Data Protection Act 1998

- Common law duty of confidentiality

Regulation of Investigatory Powers Act 2000

Ancillary to their provision ICT facilities the Governing Body asserts the employer's right to monitor and inspect the use by staff of any computer or telephonic communications systems where there are grounds for suspecting that such facilities are being, or may have been, misused.

This policy applies to all school stakeholders whilst on school premises or during any off site school activities such as trips, after school clubs or competitions:

- Governors
- Staff
- Pupils
- Parents
- Visitors

Appendix 1

ICT Acceptable Usage Agreement (AUA)

Rules for Staff, Visitors and Pupils

The computer system is owned by the school. This ICT Acceptable Use Agreement (AUA) helps to protect pupils, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

Irresponsible use may result in the loss of Internet access and could lead to disciplinary proceedings for staff.

Network access must be made via the user's authorised account and password, which must not be given to any other person.

School computer and Internet use must be appropriate to the pupils's education or to staff professional activity.

Copyright and intellectual property rights must be respected.

E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.

Users are responsible for e-mail they send and for contacts made.

Anonymous messages and chain letters are not permitted.

The use of unauthorised chat rooms is not allowed.

The school ICT systems may not be used for private purposes, unless the Executive Headteacher or Head of Schools has given permission for that use.

Use for personal financial gain, gambling, political purposes or advertising is not permitted.

ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.