

**E-Safety Policy**

**Reviewed: September 2018**

**Next Review: September 2019**

**Introduction**

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 or monitored. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Music Stuff 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 classroom.

Both this policy and the Acceptable Use Agreement (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, digital video equipment, etc); and technologies owned by staff, but brought onto school premises (such as laptops, mobile phones and camera phones).

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other E-Safety-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the head teacher believes it contains any material that could be used to bully or harass others.

The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate E-Safety behaviour that take place out of school.

**Official Guidance**

[**Guidance for Safer Working Practices for Adults who work with Children and Young**](http://www2.kirklees.gov.uk/childrenandfamilies/teachersAndGovernors/pdf/Safer-Working-Practices.pdf)

[**People prod**](http://www2.kirklees.gov.uk/childrenandfamilies/teachersAndGovernors/pdf/Safer-Working-Practices.pdf)**uced by DCSF in Jan 2009 and still current**

This guidance provides clear advice on appropriate and safe behaviours for all adults working with children in paid or unpaid capacities, in all settings and in all contexts

**Roles & Responsibilities**

As E-Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety co-ordinator in our school is Matthew McCann who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the E-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection), Childnet, UK Safer Internet Centre and Prevent Radicalisation.

Senior Management and Governors are updated by the Head/ E-Safety co-ordinator, and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school’s acceptable use agreements for staff, governors, pupils and visitors (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, safeguarding, behaviour for learning (including the anti-bullying) policy, and prevent radicalisation**.**

**E-Safety skills development for staff**

* Our staff receive information and training on E-Safety issues in the form of staff meetings, internal training, external (online) training, and emailed correspondence.
* New staff receive information on the school’s 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 to report the misuse of technology by any member of the school community to the E-Safety co-ordinator or the Headteacher.
* All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.

**Managing the school E-Safety messages**

* We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used.
* The E-Safety policy will be introduced to the pupils at the start of each school year.

**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.

* The school provides opportunities within a range of curriculum areas to teach about E-Safety.
* Issues relating to E-Safety are addressed regularly in centre (pupil) meetings.
* Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
* Pupils are 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/ Childnet/ CEOP report abuse button.
* Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models and discussions.
* Spiritual, Moral, Social and Cultural education is imbedded within our PSHE/Citizenship curriculum, which aims to promote British Values, and prevent radicalisation.

**Managing the Internet**

**Use of the Internet to Enhance Learning:**

* The school internet access is designed for pupil use and includes (specialised) filtering.
* Pupils are taught what internet use is acceptable and what is not.
* Internet access will be planned to enrich and extend learning activities.
* Staff will preview any recommended sites before use.
* Staff will guide pupils in on-line activities that will support learning outcomes planned for the pupils’ age and ability.
* Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.
* Respect the work and ownership rights of people outside the school, as well as other pupils or staff. This includes abiding by copyright laws.

**Authorised Internet Access**

* All staff must read and sign the ‘Acceptable Use Agreement’ before using any school ICT resource.
* Parents are asked to sign and return a consent form for pupil access.
* Pupils must reading and sign the ‘Pupil Acceptable Use Agreement’ before using any school ICT resource.

**World Wide Web**

* If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the headteacher or E-Safety co-ordinator.
* School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
* Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
* Anti-virus protection is installed and kept up to date on all school machines.

**Social Networking Sites**

The use of public social networking sites (e.g. bebo, myspace, facebook & Twitter) is not allowed in school unless this is specifically required for coursework.

* School will block/filter access to social networking sites and newsgroups unless a specific use is approved.
* Pupils will be advised never to give out personal details of any kind which may identify them or their location.
* Pupils are taught not to place personal photos on any social network space.

Staff should ensure that:

* No reference should be made in social media to pupils / pupils, parents / carers or school staff
* They do not engage in online discussion on personal matters relating to members of the school community
* Personal opinions should not be attributed to the school or local authority
* Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

**Mobile technologies**

* The school allows staff to bring in personal mobile phones and devices for their own use. Only in exceptional circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device. If a personal device is used a log sheet must be completed. Please see appendices.
* Staff are not permitted to use mobile phones / texts during lesson time.
* The school is not responsible for the loss, damage or theft of any personal mobile device.
* The sending of inappropriate text, photo or video messages between any member of the school community is not allowed.

**Managing email**

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. 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 international. We recognise that pupils need to understand how to style an email in relation to their age and good ‘etiquette’.

The school provides all staff with their own email 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. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This account is to be used for all school business.
* Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
* Pupils may only use approved e-mail accounts on the school system.
* Pupils must immediately tell a teacher if they receive offensive e-mail.
* Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
* Access in school to external personal e-mail accounts may be blocked.
* Pupils must not have access to school email unless it is specifically for coursework.

**Safe Use of Images**

* With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
* Staff are permitted in exceptional circumstances to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips but on return to school they must transfer the images and delete them from their personal devices.
* Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

**Publishing pupil’s images and work**

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

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

Published content and the school website and learning platform.

* Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
* Pupils’ full names will not be used anywhere on the website or blog, especially in association with photographs.
* Written permission from parents or carers will be obtained annually which will consent to photographs of pupils being published on the school website.

**CCTV**

* The school uses CCTV for security and safety. The only people with access to this are the Headteacher, SLT & centre managers. Notification of CCTV use is displayed at the front of the school.

**Webcams**

* Some webcam sites may contain, or have links to, inappropriate or adult material.
* Teachers must always view any webcam sites or listings before allowing pupils to do so.
* Pupils are alerted to the danger of using web cams as an extension of a chat room.
* Although this will be highly unlikely at school, pupils need to know the risks involved when using webcams at home.

**Managing Emerging Technologies**

Emerging technologies will be examined by the E-Safety officer for educational benefit and a risk assessment will be carried out before use in school is allowed.

**Filtering, Monitoring and Internet Security**

Music Stuff’s internet access is designed for whole school use and includes filtering appropriate to the user group (staff, administration, pupil and visitor). Internet use, at Music Stuff, is filtered on two levels. First level filtering is provided by McAfee filtering software. The second level of filtering is provided by K9 filtering software. This second level of filter can be provided instantly.

Music Stuff will take all reasonable precautions to ensure that users only access appropriate material. However due to the international scale and nature of the internet it is not possible to ensure that inappropriate material will never appear on a school computer.

The school will work with the local authority, DFE and the Internet Service Provider to ensure that filtering systems are fully functional and live to protect pupils and will regularly review the systems in place and improve them when necessary to provide safe, secure and robust access to online resources. If staff or pupils discover an inappropriate site it should be reported to the E-Safety lead immediately.

The school ICT systems will be reviewed regularly. Virus protection will be updated regularly and advice on security strategies from external sources will be discussed and implemented as necessary.

Activities regarding computer/network usage/access may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current data protection guidelines.

Such records and information are sometimes required - under law - by external agencies and authorities. Music Stuff will comply with such requests when formally submitted.

**Protecting Personal Data**

Personal data will be recorded, processed, transferred and made available according to the

Data Protection Act 1998. Please see the Music Stuff ‘Data Protection Policy’ for more information.

**Equal Opportunities**

**Pupils with additional needs**

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.

**The Prevent Duty 2015**

The statutory guidance makes clear the need for schools to ensure that children are safe from radicalisation and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place, Music Stuff uses K9 software, and McAfee Live to monitor pupils’ online activity with procedures for investigating any misuse, in place.

As with other online risks of harm, every member of staff needs to be aware of the risks posed by the online activity of extremist and radicalisation groups; this is entrenched within annual Safeguarding Training.

**Handling E-Safety Complaints**

* Complaints of Internet misuse will be dealt with by the E-Safety Ofifcer or Headteacher and recorded in the Incident Log (see appendices).
* Any complaint about staff misuse must be referred to the Headteacher.
* Complaints of a child protection nature must be reported to the Designated Safeguarding Lead (Matthew McCann), or in his absence, one of the Deputy Safeguarding Officer’s (Daniel McCann, Lenny Portersmith).
* Pupils and parents will be informed of the complaints procedure.
* Pupils are encouraged to inform their teacher or other adults in school regarding anything which makes them feel uncomfortable while using ICT.

**Breaches of this Policy**

Incidents which are determined to be in contravention of the E-Safety policy, or reasonable use policy, will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

It is not possible to provide an exhaustive list of potential ways in which a user may contravene this policy but in general such breaches will be categorised into one of three levels of severity and each level of breach will carry with it a possible range of sanctions, consequences and/or penalties.

In the event a Portable Computer is damaged or lost as a result of non-compliance with this policy or as a result of other negligent action, then you may be required to make a full or partial contribution towards any reparation/replacement costs, at the discretion of Music Stuff.

**Minor Breach**

This level of breach will attract a verbal warning. In general, this category will relate to behaviour or misuse of computer facilities that can be characterised as disruptive or a nuisance. Examples of this level of non-compliance would include:

* Taking food and/or drink into ICT facilities where they are forbidden.
* Sending nuisance (non-offensive) email
* Behaving in a disruptive manner.

Not all first offences will automatically be categorised at this level since some may be of a significance or impact that elevates them to one of the higher levels of severity.

**Moderate Breach**

This level of breach will attract more substantial sanctions and/or penalties. Examples of this level of non-compliance would include:

* Repeated minor breaches within the above detailed 12-month period.
* Unauthorised access through the use of another user’s credentials (username and password) or using a computer in an unauthorised area.
* Assisting or encouraging unauthorised access.
* Sending abusive, harassing, offensive or intimidating email.
* Maligning, defaming, slandering or libelling another person.
* Misuse of software or software licence infringement.
* Copyright infringement.
* Interference with workstation or computer configuration.

**Severe Breach**

This level of breach will attract more stringent sanctions, penalties and consequences than those above,

and access to computing facilities and services may be withdrawn (email account suspension) until the

disciplinary process and its outcomes have been concluded. Examples of this level of breach would include:

* Repeated moderate breaches.
* Theft, vandalism or willful damage of/to ICT facilities, services and resources.
* Forging email i.e. masquerading as another person.
* Loading, viewing, storing or distributing pornographic or other offensive material.
* Unauthorised copying, storage or distribution of software.
* Any action, whilst using Music Stuff computing services and facilities deemed likely to bring the Music Stuff into disrepute.
* Attempting unauthorised access to a remote system.
* Attempting to jeopardise, damage circumvent or destroy ICT systems security.
* Attempting to modify, damage or destroy another authorised users data
* Disruption of network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities.

**Process**

An investigation will be carried out, in confidence, by Music Stuff Leadership under the direction of the Headteacher. This report may be used throughout and to inform the disciplinary process.

**Communication of Policy**

Pupils

* Rules for Internet access will be posted in all computer rooms.
* Pupils will be informed that Internet use will be monitored.
* Pupils will sign an acceptable usage policy before being allowed access to computers.

Staff

* All staff will be provided with a copy of the School E-Safety Policy and its importance explained.
* Staff are made aware that Internet traffic is monitored by the use of specialised software and is traced to the individual user. Discretion and professional conduct is essential at all times.
* Staff will be expected to use an acceptable usage policy before being able to use any ICT equipment.

Parents

* Parents’ attention will be drawn to the School’s E-Safety Policy in newsletters, pre-admit, and school website.
* Parents will receive a consent/letter in reference to the E-Safety regulations.

Helpful websites [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk/) [www.chatdanger.com](http://www.chatdanger.com/) [www.getsafeonline.org](http://www.getsafeonline.org/)

<https://www.tamesidesafeguardingchildren.org.uk/>

**Reviewing this Policy**

**Review Procedure**

There will be an on-going opportunity for staff to discuss with the E-Safety coordinator any issue of E-Safety that concerns them.

This policy will be reviewed annually and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

**Pupil Acceptable Use**

**Agreement / E-Safety Rules**

* I will only use ICT in school for school purposes.
* I will only use my class email address or my own school email address when emailing.
* I will only open email attachments from people I know, or who my teacher has approved.
* I will not tell other people my ICT passwords.
* I will only open/delete my own files.
* I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
* I will not deliberately look for, save or send anything that could be
  + unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
* I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
* I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
* I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E-Safety.

Print……...…………………………………….

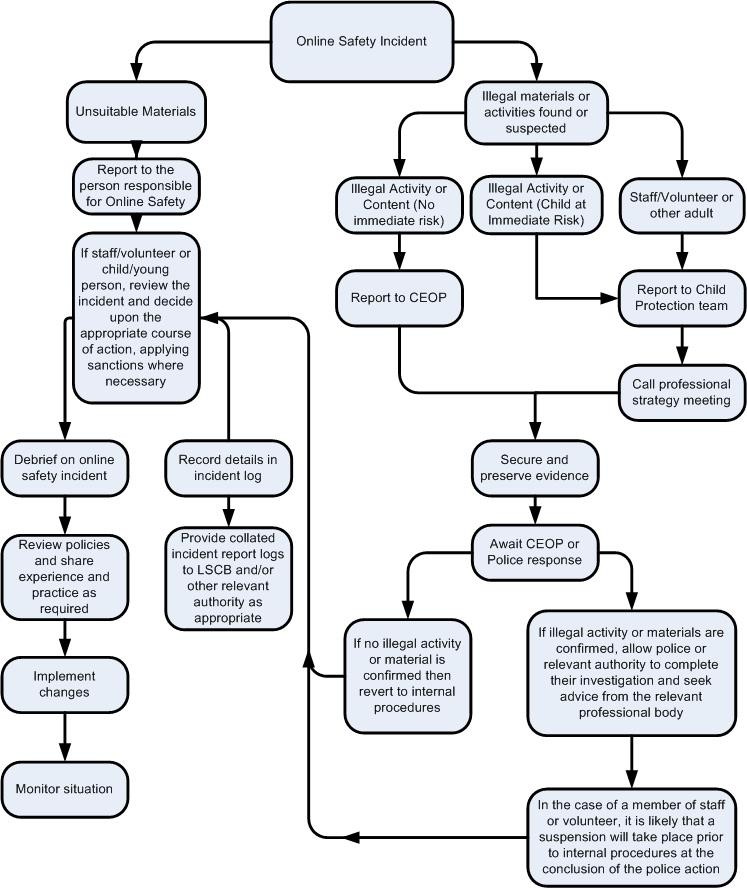
Signed………………………………………….

Date……………………………………………..

**Illegal Incidents (Online)**

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart for responding to online safety incidents and report immediately to the E-Safety officer.

A CEOP referral button (link) is available at the top of the school website. [**www.musicstuffeducation.org**](http://www.musicstuffeducation.org)**.** Children, parents and staff can use this to report concerns about online sexual exploitation, grooming and abuse.



**Appendix A**

**School E-Safety Log**

Details of  **ALL** E-Safety incidents are to be recorded to the E-Safety Coordinator. This will be monitored termly by the headteacher, member of SLT or chair of governors.

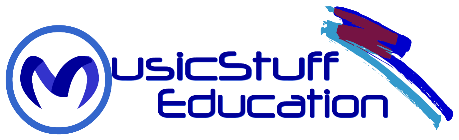
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date &**  **Time** | **Name of Pupil or Staff Member** | **Male/**  **Female** | **Room and Computer/Device** | **Details of Incident (Including Evidence)** | **Actions & Reasons** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Appendix B**

**Use of Personal Device Log**

Details of  **ALL** calls to parents/carers on personal devices are to be recorded to the E-Safety Coordinator. This log will be monitored termly by the headteacher, member of SLT or chair of governors.

|  |  |  |
| --- | --- | --- |
| **Date & Time** | **Name of Member of Staff** | **Details of Contact** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |



Music Stuff Education

Unit 2 – The Cuthbert Centre

(Entrance via Bartlett Street)

877 Ashton Old Road

Manchester

M11 2NA

2017-2018

Dear Parent/Carer

ICT including the Internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these E-Safety rules with your child and return the slip at the bottom of this page. If you have any queries or require further information, please contact your child’s class teacher

Yours sincerely



M McCann

Headteacher

The E-Safety rules have been discussed and …………………………………….......... (child name) agrees to follow the rules and to support the safe use of ICT at School.

Pupil signature :……………………………………………………………………………………..

Parent/Guardian Signature:…….………………….…………………………………………….….

Date:…….………………….…………………………………………….….