COMPANY NUMBER 10385941

E-Safety Policy

September 2024

Headquarters: Moor House Adventure Centre; Rainton Gate, West Rainton, Houghton le Spring, Tyne & Wear. DH4 6QY.

Tel: 01915841703 (Opt. 5) Mob: 07792834117 Email: abworld365@gmail.com Web: www.worlds.org.uk

Introduction

New technologies have become integral to the lives of children and young people in today's' society, both within school and in their lives outside school.

In alignment with our overall mission and as facilitators of learning, we believe that technology is a powerful tool that creates unique and relevant instructional experiences providing enriching, engaging, and varied sensory engagements that ultimately enhance the learning process. Technology is developing at an increasingly rapid rate and at World Alternative Education Limited we are committed to nurturing active, lifelong learners preparing them to be responsible, contributing members of society and global citizens who can use technology as a tool to help shape their lives and their communities.

We believe that technology initiatives will provide powerful resources, with which students will engage in challenge based meaningful learning that will encourage them to analyse collaborate, discover and create thus preparing them to become responsible citizens of the digital world.

These elements, we believe, are vital in all areas of a child's education. In a digital world, however, there is a need for our learners to be able to use technology to present information, communicate and discover.

At World Alternative Education Limited we expect that a students learning environment contributes to the development of these skills and that all students have access to suitable, up to date equipment that enables learning to take place anywhere/anytime and in any place.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in school are bound.

The company's e-safety policy aims to ensure safe and appropriate use. The development and implementation of such a strategy will involve all members of the community and the students themselves.

We acknowledge in this policy that the use of new digital technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

1. Access to illegal, harmful or inappropriate images or other content
2. Unauthorised access to/loss of/sharing of personal information
3. The risk of being subject to grooming by those with whom they make contact on the internet
4. The sharing/distributing of personal images without an individual's consent or knowledge
5. Inappropriate communication/contact with others including strangers
6. Cyber-bullying
7. Access to unsuitable video/internet games
8. Plagiarism and copyright infringement
9. Illegal downloading of music or video files
10. The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situation in the offline world and it is essential that this e-safety policy is used in conjunction with other school policies (e.ge. anti bullying, behaviour and attendance and child protections policies)

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these.

Our company must demonstrate that they have provided the necessary safeguards to help ensure that they have done everything reasonable expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

This policy applies to all members of the company (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are user of ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers head teachers (in this case director and managers) to such extent as is reasonable to regulate the behaviour of students 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 cyber bullying, or other e-safety incidents membership of the school.

The company will deal with such incidents within this policy and associated behaviour and anti bullying policies and will, where know, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Director

1. The Director is responsible for ensuring the safety (including e-safety) of members of the company by taking on the role of the e-safety officer.
2. The Director is responsible for ensuring that the e-safety officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as necessary.
3. The Director will ensure that there is a system in place to allow for monitoring and support those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.
4. The Director and at least one other member of staff should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Officer

1. Takes day to day responsibility for the e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents with the digital leaders and technical support.
2. Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
3. Provides training and advice for staff.
4. Liaises with the local governing body safeguarding committee.
5. Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
6. Attends relevant meeting.
7. Will investigate breaches of e-safety and communicate with the respective members of staff with regards to sanctions.

Designated safeguarding lead(s) for child protection will be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

1. Sharing of personal data
2. Access to illegal inappropriate materials
3. Inappropriate online contact with adults/strangers
4. Potential or actual incidents of grooming
5. Cyber bullying

Students

1. Are responsible for using the school ICT systems in accordance with the student acceptable use policy, which they will be expected to sign before being given access to systems.
2. Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
3. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
4. Will be expected to know and understand company policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand company policies on the taking/use of images and on cyber bullying.
5. Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school.

Parents

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT that their children. The company will therefore take every opportunity to help

parents understand these issues through parents' evening, newsletters, website/VLE and information about national local e-safety campaigns/literature.

Education and Training

1. Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need to help and support of the school to recognise and avoid e-safety risks and build their resilience.

e-safety education will be provided in the following ways:

1. A planned e-safety programme will be provided as part of PDE and should be regularly visited – this will cover both the use of ICT and new technologies in school and outside school.
2. Key e-safety message will be reinforced in PDE and at breakfast time.
3. Students should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
4. Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school. Students will be encouraged to access school policies regarding e-safety and taught the importance of adhering to such policies.
5. Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
6. Staff should act as good role models in their use of ICT, the internet and mobile devices.

2. Education – parents/carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on line experiences. Parents often either underestimate or not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. 'There is a generational digital divide' (Byron Report: http://webarchive.nationalarchives.gov.uk/20101021152907/http://publications.education.gov.uk/default.aspx?pagefunction=productdetails&pagemode=publications&productid=dcsf-00334-2008&).

The school will therefore seek to provide information and awareness to parents and carers through:

1. Regular digital learning event for parents.

2.Education & Training – staff

It is essential that all staff receive regular e-safety training and understand their responsibilities, as outlined in this policy:

Training will be offered as follows:

1. A planned programme of formal e-safety training will be made available to staff.
2. All new staff will receive e-safety training as part of their induction programme ensuring that they fully understand the school e-safety policy an acceptable use policies.
3. The e-safety officer will receive regular updates through attendance at LA/other information/training sessions/safeguarding first and by reviewing guidance documents released by LA and others.
4. This e-safety policy and its updates will be presented to and discussed by staff in staff meetings/digital leader meetings.

Technical – Infrastructure/Equipment, Filtering and Monitoring

The company will be responsible for ensuring that the infrastructure/network is as safe and secure as is reasonable possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

1. The company's ICT systems are managed to ensure that the company meets the e-safety technical requirements.
2. There are regular reviews and audits of the safety and security of company ICT systems.
3. Server, wireless systems and cabling are securely located and physical access restricted.
4. All users have clearly defined access rights to school ICT systems.
5. All users are provided with a username and password.
6. That 'administrator' passwords for the company ICT system must also be available to the Director and kept in a secure place (e.g. company safe).
7. Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
8. Any filtering issues are reported immediately to e-safety officer.
9. Requests from staff are sites to be removed from the filtered list are considered by the ICT technical e-safety officer. If the request is agreed, this action will be recorded and logs of such action shall be reviewed regularly.
10. Remote management tools cannot be used by staff to control workstations and view user's activity.
11. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices from accidental or malicious attempts which might threaten the security of the school systems and data.
12. Agreed protocols are in place for the provision of temporary access of 'guests' (e.g. trainee teacher, visitors) other the school system. Passwords will be changed following use of an account.
13. Agreed protocols are in place that forbids staff from installing programmes on workstations/portable devices.

14. Agreed protocols are in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school workstations/portable devices. Staff should not use memory sticks or external drives to remove personal student data.
15. The infrastructure and individual workstations are protected by up to date virus software.
16. Risk assessments are completed prior to any major network/digital technology advancement or change.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety measures in the use of ICT across the curriculum.

1. In lessons where internet use is pre planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
2. Where students are allowed to freely search internet e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit. Students should be made aware that all content is filtered and monitored.
3. It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT team can temporarily remove those sites from the filtered list for the period of study (where possible). Any request to do so, should be auditable, with clear reasons for the need.
4. Students should be taught in all lessons to be critically aware of the material/content they access online and be guided to validate the accuracy of information.
5. Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Mobile and Digital Technology

Access to mobile/digital technology is developing at an increasingly rapid rate and at World Alternative Education Limited we are committed to nurturing active, lifelong learner preparing them to be responsible, contributing members of society and global citizens who can use technology as a tool to help shape their lives and their community. At World Alternative Education Limited we expect that a student's learning environment contributes to the development of these skills and that all pupils have access to suitable, up to date equipment that enables learning to take place anywhere/anytime and in any place.

Mobile Phones

Mobile Phones are not permitted to be kept by students during the day at World Alternative Education. They will be collected during breakfast, stored safely and returned to students at the end of the school day. Young people may be permitted to keep mobile phones during 1-1 sessions and will have access in supported living.

Mobile phones used in the right context can be an effective tool in education. Most young people use their mobile phones for many purposes. To embrace their interest these devices we need to give them the opportunity to use this tool to support their learning. Students have access to a number of inbuilt tools from calendars, notepads, email system, cameras, voice recorders etc. to benefit the use of these tools mobile phones can be used in lessons providing the teacher is comfortable and can see the purpose.

Mobile phones should not be used to make calls, texts or use the camera/video in an inappropriate manner. Students should be given clear guidelines on what is expected and what is classed as acceptable use. If teachers feel uncomfortable with these tools in operation students should be asked to put them out of sight in their bags/pockets. Use of 'bluetooth/3g/4g/5g' should be avoided unless there is a purpose for sharing files in this manner. Hot spotting is not permitted.

Use of digital and video images – photographic, video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reports of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

1. When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images in particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
2. Staff are allowed to digital/video images to support education aims, but must follow school policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purpose.
3. Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individual or the school into disrepute.
4. Students must not take, use, share, publish or distribute images of others without their permission.
5. Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
6. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
7. Written permission from parents or carers will be obtained when each students joins the company.
8. Student's work can only be published with the permission of the student and parents or carers.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the company considers the following as good practice.

1. Users need to be aware that email communications may be monitored.
2. Users must immediately report, to the e-safety officer or director, in accordance with the company policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
3. Any digital communication between staff and students or parent/carers must be professional in tone and content. These communications may only take place on official (monitored) systems. Personal email addresses or public chat/social networking programmes must not be used for these communications.
4. Students should be taught about email safety issues, such s the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
5. Personal information should not be used to identify members of staff.

Responding to Incidents of Misuse

It is hoped that all members of the company will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless of irresponsible or, very rarely, apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

1. Child sexual abuse images.
2. Adult material which potentially breaches the Obscene Publications Act.
3. Criminally racist material.
4. Other criminal conduct, activity or materials.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are use to investigate preserve evidence and protect those carrying out the investigation.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate

5. Kept no longer than is necessary
6. Processed in accordance with the data subject's rights
7. Secure
8. Only transferred to other with adequate protection.

Staff must ensure that they:

1. At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
2. Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged off' at the end of any session in which they are using personal data.
3. Transfer data using encrypted or secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

1. The data must be encrypted or password protected
2. The data should not include personal details with regard to students
3. The device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected).
4. The device must offer approved virus and malware checking software.
5. The data must be securely deleted from the device, in line with the school policy once it has been transferred or its use is complete.

Policy Review

This policy will be reviewed annually or in light of any changes in legislation and/or guidance.

This policy document will be reviewed in September 2025.

Signed by:

Martin Coy (General Manager)

MCoy