E-SAFETY POLICY

Date Approved by Governors	January 2023
Review Date	June 2024
On behalf of Governors signed	Signed copy on file
Print name	
Print name	
Principal's signature	

All One In A Million Free School Policies have been devised to ensure that:

- OIAM core values are at the heart of all we do: compassion, honesty, integrity and excellence
- Students from all backgrounds and all abilities are welcome
- Each student has the opportunity to flourish and achieve or exceed their potential
- We value the individuality of each student within the context of membership of our community
- We are committed to raising educational attainment and improving our students' life chances
- We provide an environment in which all students will be self-aware, self-disciplined and confident
- All students will understand how to make a positive contribution to our community
- We support academic, creative and personal achievement through our focus on Sport, the Arts and Enterprise.

Introduction

One In A Million Free School (OIAMFS) recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

OIAMFS is committed to ensuring that all its students will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents/carers, are educated as to the risks that exist so that they can take an active part in safeguarding children.

The nominated senior person for the implementation of the School's e-Safety policy is the Deputy Vice Principal.

The curriculum requires students to learn how to locate, retrieve and exchange information using ICT. Teachers need to plan to integrate the use of communications technology such as web- based resources and email. ICT skills are vital to access life-long learning and employment. Technologies present risks as well as benefits. Internet/social networking use for work, home, social and leisure activities is expanding in all sectors of society. This brings students into contact with a wide variety of influences, some of which may be unsuitable. Unmediated Internet access through computers, telephones, i-pads etc. brings with it the possibility of placing students in embarrassing, inappropriate and even dangerous situations (Refer to OIAMFS Safeguarding Policy).

Whole school approach

All members of the school community have a responsibility for promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. This includes vigilance when children are accessing the internet at school to ensure that they do not access inappropriate websites. As such, parents, students, staff, governors and visitors are required to agree to and sign an acceptable use agreement/code

All staff should be familiar with the school's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras

- procedures in the event of misuse of technology by any member of the school community
- their role in providing e-safety education for students.

- publication of student information/photographs on the school website

Staff are reminded/updated about e-safety regularly and new staff and students receive information on the school's acceptable use policy as part of their induction. In September of each new school year, all OIAM students participate in dedicated teaching and learning activities about E-safety.

Core Principles

- Guided Educational Use – curriculum internet use should be planned, task-orientated and educational within a regulated and managed environment.
- Risk Assessment – students must be protected from danger (violence, racism, exploitation) and learn how to recognise and avoid it.
- Responsibility – all staff, governors, external providers, parents/carers and students must take responsibility for the use of the Internet.
- Regulation – in some cases eg. unmoderated chat rooms, immediate dangers are presented and their use is banned. In most cases strategies on access must be selected and developed to suit the educational activities and their effectiveness monitored.
- This policy is closely related to the guidance contained in;
  Keeping Children Safe In Education – statutory guidance to schools and colleges (DfE September 2019).
- With regard to Radicalisation via the internet and social media, the school fully adopts The Prevent Duty – advice for schools and childcare providers (DfE June 2015).

Importance/Benefits of Internet Use

- Raise educational standards, promote student achievement.
- Support work of staff and enhance management systems.
- Part of the curriculum and a necessary tool in teaching and learning.
- Students are entitled to quality Internet access as part of their 21st century learning experience.
- Access to worldwide resources and experts.

- Educational and cultural exchanges between students worldwide.
- Facilitate staff professional development.
- Communication with external services.
- Exchange of curriculum and administrative data/sharing of good practice.

Ensuring Internet use Enhances Learning

- Internet access will be designed expressly for student use and will include filtering appropriate to students' ages.
- Students will be taught what is acceptable and what is not acceptable and given clear learning objectives when using the Internet.
- Internet use will be planned to enhance and enrich learning. Access levels and online activities will be provided and reviewed to ensure they reflect curriculum requirements and student age.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Student Evaluation of Internet Content

- Any user discovering unsuitable sites must report the address and content to a teacher, Learning Support Assistant or the Designated Safeguarding Leads as appropriate.
- The use of Internet derived materials must comply with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

Management of Email

The use of email within school is an essential means of communication for staff. 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 student based, within school, between schools or internationally. We recognise that students need to understand how to style an email in relation to their age.

- Students may only use approved email accounts on the school system and only under direct teacher supervision for educational purpose.
- Students must immediately tell a teacher if they receive offensive email.

- Students must not reveal details such as address/telephone number of themselves or others or arrange to meet anyone in email communication.
- Social email can interfere with learning and will be restricted.
- Email sent to an external organisation should be carefully written and authorised by a teacher before sending.

- The school gives staff 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.
- Under no circumstances should staff contact students or parents using personal email addresses.
- All students must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Staff must inform a member of SLT if they receive any offensive or inappropriate emails.

Management of the School Website Content

- The point of contact on the website should be the school address, email and telephone number. Staff and students' home information will not be published.
- Use of photographs showing students and students' names will not be used on the website without parental consent.
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Social Networking

- Students will not be allowed access to public or unregulated chat rooms, social networking sites and forums.
- Students may only use regulated chat environments and forums – this use will be supervised, whenever possible, and the importance of chat room safety emphasised.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed.
- Mobile phones will not be used during lessons (or the rest of the school day) unless they provide a benefit to a student's education.
- The school's video cameras may be used by students for educational use.

Authorisation of Internet Access

All Internet access is monitored and recorded using electronic means.

- Inappropriate use of the Internet will be dealt with in accordance with the school's Behaviour Policy.

Risk Assessment

- Some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure such material is not accessed by students. However, it is not possible to guarantee that such material will never appear on an school computer – OIAMFS cannot accept liability for material accessed or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risk will be reviewed regularly.

Management of Filtering

- The school will work in partnership with parents/carers, the DFE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- Any Internet user must report unsuitable/illegal sites to the Network Manager (and the Designated Safeguarding Lead if necessary) immediately.
- The Network Manager will oversee regular checks to ensure that the filtering methods used are appropriate, effective and reasonable. Content is filtered using 'Light Speed' and 'FortiGate' and communications are monitored through 'AB Tutor'.
- If filtered websites need to be used by staff, they must inform ICT Technicians to have them unblocked for a set period of time (requests need to be approved by the Line Manager).

ICT System Security

- The school's ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Files held on the school's network will be regularly checked.
- Use of portable media such as memory sticks and CD will be reviewed regularly.
- Downloading of unauthorised files will be prohibited, and where possible blocked.
- Use of the school's ICT systems will be subject to the Data Protection Act and the Computer Misuse Act.

Mobile Phones

OIAMFS recognises that mobile phones can play a significant role in keeping students safe not least because of the contact it offers to parents/carers. This is particularly true in winter when students are going home in the dark. What is more OIAMFS recognises that a mobile phone is often the possession that students value the most.

However, given OIAMFS's ICT provision and in particular the use of iPads it is inconceivable not likely that a student would ever need to use a mobile phone in OIAMFS. With that in mind, it is expected that EVERY student switches off their mobile phone and leaves it in their bag or locker until they leave school at the end of the day.

Occasionally students tell us they need access to a phone because they are awaiting important news from a parent or carer. If this is the case it is the expectation of OIAMFS that the parent/carer ring OIAMFS reception and that information will them be passed on sensitively to the student.

Students who violate this rule will be dealt with in accordance with OIAMFS's behaviour policy. Whilst OIAMFS recognises that staff may have to use a mobile phone as part of their role within OIAMFS, nonetheless, it expects them to be good role models. To that end staff must not use mobile phones in a public place in school.

Unacceptable Activity

- Wasting staff effort or networked resources, including time on end systems accessible via the network and the effort of staff involved in support of those systems
- Corrupting or destroying other users' data
- Violating the privacy of other users
- Disrupting the work of other users
- Using the network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
- Continuing to use an item of networking software or hardware after OIAMFS has requested that use cease because it is causing disruption to the correct functioning of OIAMFS
- Other misuse of the OIAMFS network, such as introduction of viruses

- Use any mobile or digital technologies 3G or mobile Internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

Cyberbullying

Cyberbullying is the use of ICT, particularly mobile phones and the internet, to deliberately upset someone else. The whole OIAM community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head teachers/Principal have the power 'to such an extent as is reasonable' to regulate the conduct of students when they are off site.

Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

Common types of cyber bullying

- Text messages – that are threatening or cause discomfort – also included here is "bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology).
- Picture/video-clips via mobile phone cameras – images sent to others to make the victim feel threatened or embarrassed.
- Mobile phone calls – silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
- Emails – threatening or bullying emails, often sent using a pseudonym or somebody else's name.
- Chatroom bullying – menacing or upsetting responses to children or young people when they are in web-based chatrooms.
- Instant messaging (IM) – unpleasant messages sent while children conduct realtime conversations online using MSM (Microsoft Messenger) or Yahoo Chat.
- Bullying via websites and social networking sites – use of defamatory blogs, personal websites and online personal "own web space" sites

Preventing Cyberbullying

It is important that the school works in partnership with students and parents to educate them about Cyberbullying as part of our e-safety curriculum. They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.
- report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.
  Additional online advice on how to react to Cyberbullying can be found on www.kidscape.org and www.wiredsafety.org

Supporting the person being bullied

Support shall be given in line with the OIAM Behaviour Policy:

- Give reassurance that the person has done the right thing by telling someone and inform parents.
- Make sure the person knows not to retaliate or return the message.
- Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages.)
- Check the person knows how to prevent it from happening again e.g. blocking contacts, changing contact details.
- Take action to contain the incident when content has been circulated: remove content, contact the host (social networking site) to get the content taken down, use disciplinary powers to confiscate phones that are being used to cyber bully – ask the student who they have sent messages to.

Investigating Incidents

All cyberbullying incidents should be recorded and investigated in the same manner as any other bullying incident. OIAM staff will investigate all incidents or concerns as fully as any other bullying incident.

Student, Staff and Parental Awareness

- All stakeholders will be made aware of this policy and how it relates to them.
- All staff will sign the Acceptable Use Agreement. See Appendices
- Students will be instructed in responsible and safe internet use before being granted access.
- Responsible use of the internet, including social networking will be discussed through the curriculum, assemblies and PHSE activities.
- The monitoring of internet use is a sensitive matter – staff who operate monitoring procedures will be supported by the Deputy Vice Principal/Principal.
- Staff training in safe and responsible internet use and on the contents of this policy will be provided as required.
- A partnership approach with parents/carers will be encouraged, with relevant information on issues covered by this policy made available.
- Cases of internet misuse and other disciplinary breaches related to the policy will be dealt with through the schools Behaviour, Bullying and Safeguarding/Child Protection Policies, as appropriate. In cases of potential radicalisation/extremism The Prevent Duty will be implemented and could involve referral of individuals to the Prevent Duty Delivery Board and the Channel Panel.

Responding to e-safety incidents/complaints

As a school, OIAM will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.

Complaints relating to esafety should be made to a member of the Senior Leadership Team. Any complaint about staff misuse must be referred to the One In A Million Free School Principal.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Principal, possibly leading to investigation, dismissal and involvement of police for very serious offences
- Students and parents will be directed to the school complaints procedure on request
- Parents and students will need to work in partnership with OIAM staff to resolve issues.

Appendix 1

ICT Acceptable Use Policy – Parental Agreement

Dear Parent/ Carer,

The use of ICT including the Internet, e-mail, learning platforms and today's mobile technologies are an integral element of learning in One In A Million Free School. In making this as successful and as beneficial as possible for all students, we expect all students to act safely and responsibly when using technology both within, and outside of, the school environment. We review our E-safety policy regularly and have just updated our Acceptable Use Policy.

The enclosed ICT Acceptable Use Policy forms part of the wider One In A Million Free School E-Safety Policy and in association with both the school's Behaviour for Learning Policy, Safeguarding Policy and Home-School Agreement, outlines those principles we expect our students to uphold for the benefit of both themselves and the wider school community. I would therefore ask that you please read and discuss the enclosed E-safety Acceptable Use Policy with your child and return the completed slip at the bottom of this page as soon as possible.

If you would like to find out more about E-safety for parents and carers, please visit the ThinkUKnow website at: www.thinkuknow.co.uk. There is a range of parental control software available online (either free or for purchase) which you may like to consider if you do not have this already.

If you have any concerns or would like to discuss any aspect of E-safety, please contact the school for further guidance.

Kind regards

J Hobbs

Principal

Appendix 2

ICT Acceptable Use Policy – IT Acceptable Use Policy for students: Agreement / E-safety Rules

- I will follow all the safety rules when using the school IT equipment and use it properly
- I will only share my user name and password with trusted adults
- I will tell an adult if I see anything that upsets me
- I will make sure that when I blog I am responsible, polite and sensible
- I will use a safe name and not my real name on the internet
- I know I am only allowed to go on the internet if my teacher has given me permission
- I will only take a photograph or video of someone if they say it is alright
- Any messages I send will be polite
- I will not deliberately write anything which upsets other people
- I understand that the school may talk to my parent or carer if they are worried about my use of school IT equipment
- I understand that if I do not follow these rules I may not be allowed to use the school computer or internet, even if it was done outside school

Parent/ Carer signature

We have discussed this and ..... (child's name) agrees to follow the eSafety rules and to support the safe use of IT

Parent / Carer Name (PRINT) .....

Parent / Carer (Signature) .....

Form ..... Date.....

Appendix 3

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in One In A Million Free School. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with a member of SLT.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to students.
- I will only use the approved, secure email system(s) for any school business.
- I will not email documents giving details of students unless on a secure system.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Governing Body.
- USB sticks containing data must be encrypted.
- I will not use or install any hardware or software without permission from the ICT Manager/member of SLT.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken with school devices, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or staff member.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
- I understand I cannot use my mobile phone to take photos of children
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Principal.

- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-safety policy and help students to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ..... Date .....

Full Name ..... (printed)

Job title: .....