Forge Integrated Primary School

E-Safety Policy

(January 2021)

Rationale

Online safety in school and elsewhere is of paramount concern. Schools play a crucial role in raising awareness of the risks, highlighting the impact of behaviour when engaging with online technologies and educating children and young people about how to act appropriately and stay safe.

Aims

At Forge IPS, we want pupils to have the opportunity to avail of all the positive benefits that come from learning, exploring and connecting with each other online. However, in doing so they need to know how to protect themselves. We aim to teach the children appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and other online technologies.

Scope of the Policy

This policy applies to all members of the School community who have access to and are users of the school ICT systems, both in and out of the School. In relation to incidents that occur during school hours, we will work with parents, staff and pupils to ensure E-Safety of all involved, apply sanctions as appropriate and review procedures.

In relation to E-Safety incidents that occur outside of school hours, the school will work with pupils and parents to keep all pupils safe and offer educative support where appropriate. E-Safety outside school hours is primarily the responsibility of the parents. If inappropriate activity occurs outside school hours with the intention of having a negative effect on any member of the School community, and this is brought to our attention, then we will liaise with parents as to an appropriate way forward. Any issues that arise inside school, as a result of E-Safety incidents outside of the School, will be dealt with in accordance with School Policies.

What is E-safety?

E-Safety is short for electronic safety. E-Safety covers not only use of the internet but also electronic communications via mobile phones, game consoles and wireless technology. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. At Forge IPS we aim to promote safe and acceptable practices for all staff and pupils.

Risk Assessment

21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity they will need to learn to recognise and avoid these risks — to become "Internet-wise" and ultimately good "digital citizens". Schools need to perform risk assessments on the technologies within their school to ensure that they are fully aware of and can mitigate against the potential risks involved with their use. Pupils need to know how to cope if they come across inappropriate material or situations online. The school risk assessments should inform the teaching and learning, develop best practice and be referenced in the school's Acceptable Use Policy.

DENI E-Safety Guidance, Circular number 2013/25

The main areas of risk for the school can be categorised as the Content, Contact and Conduct of activity.

CONTENT

- Access to illegal, harmful or inappropriate images or other content.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.

CONTACT

- Inappropriate communication / contact with others, including strangers.
- The risk of being subject to grooming by those whom they may make contract on the Internet.
- Cyber-bullying.

- Unauthorised access to / loss of / sharing of personal information.

CONDUCT

- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The sharing / distribution of personal images without an individual's consent or knowledge.

Many of these risks reflect situations that occur offline and it is essential that this E-Safety policy is used in conjunction with other School policies eg. Positive Behaviour, Child Protection, Anti-Bullying and Acceptable Use.

Cyber Bullying

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi- player gaming sites.
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with the School's Anti-Bullying and Discipline Policies.

If any user experiences or witnesses anything which they believe may be an e-safety issue they should report this to the school immediately.

Roles and Responsibilities

UICT Coordinator

It is the role of the UICT Coordinator to keep well- informed of current E-Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and the Childnet. The UICT Coordinator has responsibility for leading and monitoring the implementation of E-Safety throughout the school.

Principal/ UICT Coordinator

The Principal/ UICT Coordinator have the responsibility to update the Senior Leadership Team and Governors with regard to E-Safety and all governors should have an understanding of the issues at our school in relation to local and national guidelines and advice.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-Safety incidents and monitoring reports.

Teaching & Non-Teaching Staff

The Teaching and Non-Teaching staff are responsible for ensuring that:

- They have read and signed the school's Staff Acceptable Use policy.
- They have a good awareness of current e-safety matters and the school's E-Safety policy.
- They report any suspected misuse or problem to the UICT Coordinator/Principal.
- All digital communication with students should be on a professional level. This should be only carried out on school systems via email through C2K or posts on Seesaw
- E-Safety issues are embedded in all aspects of the curriculum and other school activities.
- They monitor ICT activity in lessons and extended school activities.

- Undertake all e-safety training organised by the school. This e-safety policy and updates will be discussed in staff meetings / INSET days.

Parents/ Carers

Parents/ Carers play an important role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate and safe way. Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to adhere to the school's E-Safety policy.

Education of Pupils

The Internet is an integral part of pupils' lives, both inside and outside school. Forge IPS seeks to enable pupils to experience the benefits of communicating online with their peers, in relative safety. To achieve this we discuss E-Safety regularly with the pupils. Age-appropriate lessons from Safer Internet Day taught and visits/presentations from local agencies such as the P.S.N.I. are organised. The school will also make use of resources from the Child Exploitation and Online Protection (CEOP), www.thinkuknow.co.uk and www.childnet.com. E-Safety posters & guidance for pupils will be placed in all classrooms. E-Safety learning is embedded into PDMU and ICT lessons. Through these activities:

- The school will promote online safety messages for pupils on how to stay safe; how to protect themselves online; and how to take responsibility for their own and others' safety.
- Pupils will be reminded to never to give out personal details of any kind which may identify them or their location on the internet.
- Pupils are informed that network and internet use will be monitored by the school and C2k.
- Pupils will learn what is appropriate and inappropriate behaviour online.
- Pupils will be able to refer to E-Safety posters around the school as reminders for safe practice.
- Pupils will know how to report an E-Safety problem.

Education of Parents and Wider Community

The school will also offer parents the opportunity to attend online safety training held by local agencies such as the P.S.N.I. The school will also promote online safety resources through publishing messages on the school's social media platform.

This policy reflects the guidance in DENI Circular 2007/1 ‘Acceptable Use of the Internet and Digital Technologies in Schools’, DENI Circular 2011/22 ‘Internet Safety’, DENI Circular 2016/26 ‘Effective Educational Uses of Mobile Digital Devices’, DENI Circular 2013/25 ‘eSafety Guidance’ and DENI Circular 2016/27 ‘Online Safety’.

To be reviewed: January 2022

FORGE INTEGRATED PRIMARY SCHOOL
EST. 1985

Childnet International

BE SMART ONLINE

S — SAFE

Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.

M — MEET

Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on **www.thinkuknow.co.uk**

A — ACCEPTING

Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.

R — RELIABLE

You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.

T — TELL

Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – **0800 11 11** or **www.childline.org.uk**

BE SMART WITH A HEART

Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.

WWW.CHILDNET.COM