E-SAFETY POLICY

Including

Acceptable Use Agreements

Our rationale-

At Imperial Avenue Infant School, we encourage pupils and staff to use technology to support teaching and learning, including access to the Internet. We also encourage and continue to explore ways of using technology to better streamline and improve our administration tasks. This E-Safety Policy for Imperial Avenue Infant School is designed to help to ensure safe and appropriate access and usage for all digital technologies across the school community.

For the purpose of this policy, digital technologies are defined as electronic tools, systems, devices and resources that generate, store or process data that can include, but are not restricted, to the following:

- Computers
- Laptops
- Websites
- Email
- Social media
- Mobile phones
- Tablets
- Blogs
- Podcasts
- Downloads
- Forums

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 online-bullying or other e-safety incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Why do we have an E-Safety Policy?

With the ever-increasing manner in the way technology is being used in education, it is paramount that as educators we have in place policies and strategies that help us to keep both staff and pupils safe. We have highly functional school-based and personal devices that give us access to powerful digital tools wherever we go. The Internet has the capacity to instantly connect us to content and to each other, but, due to its vast nature and relative immaturity as a medium, also presents unprecedented levels of risk to young people. Some of the dangers pupils may face include:

- Access to illegal, harmful or inappropriate content
- Access to content that promotes extremism and/or radicalisation
- Losing control over personal information/images
- The risk of being groomed by those with whom they make contact, exposing them to physical and sexual risk
- Exposure to, or engagement in cyber-bullying

- An over-reliance on unreliable sources of information and an inability to evaluate the quality accuracy and relevance of information on the Internet

Other school policies

This policy should be read in conjunction with other relevant school policies:

- Electronic communication guidance for staff
- Safeguarding Policy
- Anti-Bullying Policy
- SRE/PSHE Policy
- Codes of Conduct
- UK-GDPR Policy

Legal frameworks

It is the user's responsibility to ensure they are compliant and work within all UK and E.U. applicable legislation in regards to the safe and legal use of ICT in schools. This includes but is not limited to the following:

- The Sexual Offences Act 2003
- The Racial and Religious Hatred Act 2006
- The Computer Misuse Act 1990
- The Police and Justice Act 2006
- Communications Act 2003
- Data Protection Act 1998
- Malicious Communications Act 1988
- Copyright, Design and Patents Act 1988
- Public Order Act 1986
- Protection of Children Act 1978
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 1997
- The Regulation of Investigatory Powers Act 2000 (RIP)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education and Inspections Act 2006
- Equality Act 2010
- Education Act 2011
- Online Safety Bill (OSB) 2023

Governor responsibilities

Governors are responsible for the approval of the E-Safety Policy, for reviewing the effectiveness of the policy and monitoring compliance with the policy. This will be carried out by the Governor, through the Computing leader with updates on any e-safety incidents. Any incidents will be reported to the full governing body.

School leadership and management responsibilities

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the DSL's in school. The Headteacher and another member of the Senior Leadership Team 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. They are responsible for ensuring that the all DSL's and other relevant staff receive suitable

training to enable them to carry out their e-safety roles and to train other colleagues as relevant.

The Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also to support those colleagues who take on important monitoring roles.

The computing leader will provide a E-Safety report for governors throughout the year, to inform them of any incidents that may have happened in school regarding E-Safety. Also, to keep them updated of any E-Safety teaching and learning that has been taking place.

The Designated Safeguarding Lead (DSL) responsibilities

Details of the school's Designated Safeguarding Lead (DSL) are set out in our Child Protection and Safeguarding Policy.

The DSL takes lead responsibility for e-safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, Computing Co-ordinator and other staff, as necessary, to address any e-safety issues or incidents
- Ensuring that any e-safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy
- Updating and delivering staff training on e-safety
- Liaising with other agencies and/or external services if necessary

Teaching and support staff responsibilities

All staff shall make themselves aware of the content of this policy and attend relevant in house e-safety training. Staff shall be responsible for contributing to the positive re-enforcement of e-safe behaviours through their day-to-day interaction with pupils and technology. All teachers will have Our 'E-safety charter' displayed in their classrooms and refer to it as necessary. Staff should act as good role models in their use of ICT, the Internet and mobile devices.

Where personal devices are allowed, all teaching staff shall ensure that pupils' use of these devices is for legitimate educational purposes and not for texting, accessing social networking sites or recording audio, video or still imagery without permission.

All members of staff are provided with a school email address. Electronic communications with students, parents/carers and other professionals will only take place via work-approved communication channels e.g. via a school-provided email address, class dojo, WEDUC or telephone number. Staff are advised to ensure that business correspondence is received to and sent from the school email address. This is to protect staff's privacy and ensure that school business is kept separate from private correspondence.
All staff have an email disclaimer notice on the end of their emails.
The disclaimer states:
This email and any attachments are sent in confidence and are not intended to be read by any person other than an intended recipient. The recipient is responsible for conducting the appropriate virus checks and whilst appropriate security measures are

in place, we give no warranty, express or implied, that this email is free of viruses or that its transmission has been secure.

If you receive this email in error, please contact us on:
office@imperialavenue.leicester.sch.uk and permanently delete this email.
Any use, copying or dissemination of this email or any information contained in it to anyone other than an intended recipient is prohibited.

Any and all communications sent to us may be monitored and/or stored by us to ensure compliance with relevant legislation, rules and policies. All communications are handled in full compliance with all data policies and current data protection legislation including, but not limited to, United Kingdom General Data Protection Regulation (UK-GDPR) and the Data Protection Act 2018. For further information, please refer to our Privacy Notice which is available on our website www.imperialavenue.leicester.sch.uk

Parents' and carers' responsibilities

Parents and carers may have 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 their children's online experiences. Parents can often underestimate how often children and young people come across potentially harmful and inappropriate material on the Internet and can be unsure about what they should do about it.

At Imperial Avenue Infant School, we will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, E-Safety leaflets, our website and other digital communications (WEDUC).
- Parents' evenings.
- Parent meetings where key information is shared and opportunities to ask questions.

System management responsibilities

The school, in conjunction with their ICT support provider and ICT technician, will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that procedures set out within this policy are implemented:

- There will be regular reviews and audits of the safety and security of ICT systems
- All users will have clearly defined access rights to the ICT systems of the school. This will be defined and accountable by the respective ICT lead/co-ordinator(s)
- Users will be made responsible for the security of their username and password; must not allow other users to access the systems using their login details; and must immediately report any suspicion or evidence that there has been a breach of security to the school's Data Protection Officer
- Staff computers and laptops are fitted with filtering and monitoring software which flag up any inappropriate words.

The administrator passwords for the ICT system must also be available to the Headteacher and kept in a secure, physical (e.g. fire safe) or electronic location software with encrypted storage. The school, in conjunction with the ICT support provider, will use a sufficient Internet filtering system to restrict access to certain materials, adhering to current government guidelines and recommendations. However, the school is aware that children must be educated in how to deal with inappropriate material.

Pupil's responsibilities

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

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. E-safety should be referenced in all areas of the curriculum and staff should reinforce e-safety messages whenever ICT is being used.

A planned e-safety programme will be provided as part of both computing and PSHE lessons and will be regularly revisited – this will cover the use of computing both in and outside school and will include:
We use technology purposefully
We use digital devices safely and responsibly
We keep personal details private
We tell a grown-up if we feel worried
We stick to what is age appropriate

Whenever the Internet is used for research, pupils should be taught to be critically aware of the content they access online and be guided to validate the accuracy of information. Children will be taught that not everything they read on the internet is real or true. It is accepted that pupils 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 a temporary removal of those sites from the filtered list for the period of study. Any request to do so should be auditable, time-limited and with clear reasons given.

Responding to incidents of abuse and misuse

At Imperial Avenue Infant School, we understand the importance of acting on reported incidents of abuse and misuse of our ICT systems in school. The incidents may involve illegal or inappropriate activities. Imperial Avenue Infant School actively encourages a safe and secure approach to the management of the incidents.

Pupils are encouraged to report any incidents immediately to a member of staff. Staff will liaise with the Senior Leadership Team and the Designated Safeguarding Lead, ICT support as necessary to investigate the alleged incident and establish evidence of any breach or wrongdoing. Staff will:

- Work with any pupils involved to resolve issues and educate users as necessary
- Inform parents/carers of the incident and any outcomes
- Where the alleged incident involves staff misuse, the Headteacher should be informed
- Outcomes of investigations will be reported to the Head teacher and to external services where appropriate (e.g. Social Services, Police Service, the Child Exploitation and Online Protection Service). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident
- Where the alleged incident involves misuse by the Headteacher, the Chair of Governors should be informed

Useful websites

www.gov.uk

In the search box at the top of the page type:

- Preventing and tackling bullying
- Searching, screening and confiscation at school
- The Prevent Duty

www.leicestershire.gov.uk

In the search box at the top of the page type:

- E-Safety

www.thinkuknow.co.uk

Thinkuknow is the education programme from CEOP, a UK organisation that protects children both online and offline.

Explore one of the six Thinkuknow websites for advice about staying safe when you are on a phone, tablet or computer.

Acceptable Use Agreement for Governors and volunteers

ICT and related technologies such as email, the Internet and mobile devices are an expected part of working life in school. This agreement is designed to ensure that Governors and volunteers are aware of their professional responsibilities when using any form of ICT.

Before becoming school ICT users, you are always asked to sign this policy and adhere to its contents. Any concerns or clarification should be discussed with the Headteacher, who is the E-Safety Co-ordinator.

General:

- I have read the school E-safety Policy
- 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 not install any hardware or software without the permission of the E-Safety lead
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner
- I will only take images of pupils and/or staff for professional purposes in line with school policy
- I will not distribute images outside the school network/learning platform without the permission of the Headteacher
- I will report any incidents of concern regarding children's safety to the E-Safety Co-ordinator, the Designated Safeguarding Lead or Headteacher

Wi-Fi/Internet use:

- I will only use the school's email/Internet/Intranet and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Headteacher or Governing Body
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I understand that all use of the Internet and other related technologies can be monitored, logged and can be made available, on request, to the Headteacher
- I understand that I am responsible for all activity carried out under my username
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely
- I will not make copies or download any school based information on my home devices
- Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or the Chair of Governors

I agree to follow this code of conduct. I understand that the sanctions for disregarding any of the above will result in removal of access to ICT infrastructure and serious infringements may be referred to the police.

Full Name

……

Signature …… Date ……...

Acceptable Use Agreement for staff

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, carers and other professionals, they are asked to sign this agreement. Members of staff should consult the E-Safety Policy for further clarification of their responsibilities.

- I understand that it is a criminal offence to use any school ICT resource for a purpose not permitted by its owner
- I understand that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email and social networking; and that ICT use may also include personal ICT devices when used for school business
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance
- I will log off or lock the computer/device I have been using when leaving it unattended
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised ICT support person
- I will not install any software or hardware without permission
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off site or accessed remotely
- I will respect copyright and intellectual property rights
- I will report any incidents of concern regarding children's safety to a Designated Safeguarding Lead or a member of the Senior Leadership Team
- I will ensure that electronic communications with pupils including email and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. I will only utilise the school email platform to communicate any school matters
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing
- The school may exercise its right to monitor the use of information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound

I agree to follow this code of conduct. I understand that the sanctions for disregarding any of the above will result in removal of access to ICT infrastructure and serious infringements may be referred to the police.

Full Name ……

Signature …… Date ……

Acceptable Use Agreement for pupils

As pupils at Imperial Avenue Infant School, we want you to enjoy using the computers within our school.
It is very important that you:

Always look after the equipment

Be **kind** to one another, **sharing** the equipment nicely and fairly

Make sure you use **kind language** when talking to others through the computer

Only use websites or play games that your teacher has **allowed** you to use

Tell your teacher if anything or anyone makes you **feel uncomfortable** or if there is a problem

Do not bring to school any mobile phone or tablet from home (unless agreed otherwise with the school).

Remember not everything you read on the Internet may be true

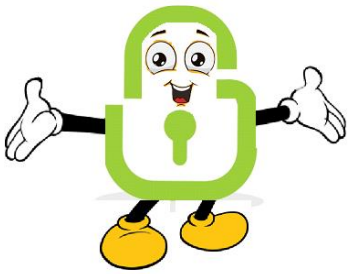
Remember that sometimes attachments can contain **viruses or bugs** so only open attachments from people you know.

I UNDERSTAND THAT THIS IS IMPORTANT, SO I PROMISE TO:

- Only use the Internet and email when an adult is nearby
- Only click on icons and links when I know they are safe
- Only send friendly and polite messages
- Never share my usernames and passwords
- Always tell an adult if I see something I don't like on a screen

My Name: ……

LOCKI SAYS KEEP SAFE



Imperial Avenue Infant School
Internet Policy

Use of the Internet, by its nature, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times, they will be able to move beyond these, to sites unfamiliar to the teacher.

The purpose of this policy is to:

- ✓ Establish the ground rules we have in school for using the Internet
- ✓ Describe how these fit into the wider context of our behaviour policy
- ✓ Demonstrate the methods used to protect the children from sites containing pornography, racist or politically extreme views and violence

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians. At Imperial Avenue Infant School, we feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Why is internet use important?

The benefits of using the internet include:

- ✓ access to a wide variety of educational resources including libraries, art galleries and museums
- ✓ world-wide communication
- ✓ gaining an understanding of people and cultures around the globe
- ✓ staff professional development through access to new curriculum materials, experts' knowledge and practice
- ✓ exchange of curriculum and administration data.
- ✓ social and leisure use
- ✓ greatly increased skills in Literacy

The school intends to teach pupils about the vast information resources available on the Internet, using it as a planned part of many lessons. All staff will review and evaluate resources available on web sites appropriate to the age range and ability of the pupils being taught. Initially the pupils may be restricted to sites which have been reviewed and selected for content. They may be given a task to perform using a specific group of web sites accessed from a common 'Favourites' menu in their web browser.

As pupils gain experience, they will be taught how to use searching techniques to locate and specific information for themselves e.g. using the phrase ‘for kids’ as the end of each search. Comparisons will be made between researching from different sources of information, (CD Rom, books, WWW). We hope that pupils will learn to decide when it is appropriate to use the Internet, as opposed to other sources of information, in terms of: the time taken; the amount of information found; the usefulness and reliability of information located. At times, information, such as text, photos etc may be “downloaded” from the Internet for use in pupils’ presentations.

How are pupils protected from inappropriate material?

To protect users from browsing inappropriate sites, our ISP (internet service provider) Wave9 uses a leading security company, Sophos, to provide internet filtering for the school. Along with internet filtering, the Sophos solution also logs all access to the internet. The filtering levels that are in place ensures that the children are safe online which are the aims of the UK Council for Child Internet Safety (UKCCIS) and adheres to the guidelines as stated in the Prevent Duty guidance which is part of the Counter-Terrorism and Security Act 2015. Any website deemed to belong to an unsuitable category by the Sophos solution will not be displayed. New websites are added and categorized constantly as the World Wide Web expands daily.

All computers on the school network have a filtering system. Children accessing the internet at school are always supervised by an adult. However it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen, so it is the responsibility of the teacher to explain the expectations of internet use to the pupils. All children in school are aware of e-safety issues and are told to turn off the screen and talk to a teacher if they ever see or read anything which they find upsetting or inappropriate. When using the computer in lessons, children ask permission to go onto the internet.

Parents have also been made aware of e-safety issues through letters being sent home. Parents are advised not to allow their children access to the internet without adult supervision.

Any inappropriate material must be reported (along with the URL) to the head teacher.

What are our expectations for the children and how are they managed?

- ✓ At Imperial Avenue, we expect all pupils to be responsible for their own behaviour on the
  Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use
- ✓ Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider can block further access to the site
- ✓ Pupils must ask permission before accessing the Internet and have a clear idea why
  they are using it
- ✓ Computers should only be used for schoolwork and homework unless permission has been granted otherwise
- ✓ No program files may be downloaded to the computer from the Internet. This to prevent corruption of data and avoid viruses
- ✓ No programs on disc or CD Rom should be brought in from home for use in. This is for both legal and security reasons
- ✓ No personal information such as phone numbers and addresses should be given out
  and no arrangements to meet someone made
- ✓ No removable media such as USB flash drives are used by the children. This is to prevent the possible spread of viruses and adhering to the Data Protection Act

- ✓ Pupils consistently choosing not to comply with these expectations will be warned,
  and subsequently, may be denied access to Internet resources

How is email managed?

Children in our school do not have access to school email. However through e-safety (within ICT lessons) they are made aware of the positives and dangers of using email, as a few children may have email accounts outside of school. They are taught how to use email safely and what to do if they feel upset or unsure about something they have read. They are taught not to hand out any personal information in an email.

All teachers have school email, which is only to be used for school purposes. This email is regulated through the EMBC network. Staff email is filtered so that any messages, originating from an external source or from another school email account that contains potentially offensive material and/or malicious programs are blocked at ISP level and will not reach the recipients. Teachers keep the passwords for these accounts secret and are the only ones with access to their account.

How is Internet access authorised?

All staff have their own login in and password, which can be used on any computer in the school. The use of the internet is monitored and there is a high level filtering system in place.

Children have access to the internet through the student log in. Each year group has a generic log in so that staff are able to review what has been saved. This also has a high level filtering system on it. Throughout the school teachers lead a demonstration using the internet and then children are allowed to use specific materials with supervision.

How are the risks assessed?

It is not possible to guard against every undesirable situation. However throughout their time in school children are constantly reminded of the dangers of the internet. They are taught many ways to use the internet safely. No child is allowed access to the internet without adult supervision. Children are constantly encouraged to tell a grownup if they see something that upsets them whether at home or at school.

The head teacher, teachers and support staff will ensure that the internet policy is being implemented effectively and methods to identify, assess and minimise risks will be reviewed regularly.