Esafety & Acceptance

Esland Isaac Newton School
Policy & Procedure

Policy	Esafety & Acceptance
Date prepared	October 2020
Review date	September 2021
Author	Rob Arrowsmith, Executive Headteacher
Signed	

Policy

This policy must be applied in the context of the school's Safeguarding (including 'Prevent'), Whistle-blowing, Staff Code of Conduct and Anti-Bullying policies. This is a whole school policy.

The primary objective of this policy is to protect all members of the school community from the adverse consequences of access to or use of all forms of electronic media where its use may result in harassment, bullying, access to inappropriate sites and people who wish to groom for sexual exploitation or radicalisation. All staff and people working at the school have an individual and corporate duty to ensure this policy is understood and is fully implemented. The use of this policy will be regularly monitored by governors in accordance with their duties and responsibilities.

Reference is made to *Keeping Children Safe in Education 2016 (KCSIE)* including the processes for referral to Children's Services, LADO (Designated Officer of the Local Authority) and/or the police where issues are identified relating to the welfare of pupils or the inappropriate conduct of staff and volunteers towards pupils through the use of technology.

Context

The Internet is an integral part of our lives and an important and useful resource for staff and pupils alike. However, like all technology there are associated risks and it is important that teachers, parents/ carers and pupils all work together to ensure usage is kept as safe as is reasonably possible.

At Esland School we believe it is essential to educate pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain safe and to act legally when using the internet and related technologies. This applies to use both in and beyond the context of the classroom.

Communication systems such as social networks, blogs, mobile phones and email have become increasingly important in our daily lives. Access to the internet can take place almost anywhere at any time and it is important that pupils, teachers and parents are aware of the risks and know how to use modern technologies appropriately. It is helpful to discuss the issues in school, at home and between friends, and to know what actions to take should

something goes wrong.

Pupils are encouraged to report any negative issues they may encounter online to a trusted adult, which includes, school staff. Students are informed how to report cyberbullying and e-safety posters are displayed in prominent positions. (See Child Protection and Safeguarding policy)

Annually, we have an e-Safety Week with relevant activities within Morning and Afternoon Reflection times, assemblies and PSHE.

All interaction is closely monitored by teaching staff and through school IT monitoring and filtering processes eg SmoothWall

ICT within school covers a wide range of functional skill development: Word, PowerPoint, Excel, Password safety, Email Protocol, Working online safely and internet e-safety. We also address the the emotional, social and legal implications of cyberbullying through our curriculum.

Staff Safeguarding professional development that includes online safety

KCSIE 2020, the school's safeguarding policy, staff code of conduct and e-safety CPD for staff all support the upskilling of staff in terms of awareness, reporting and dealing with online safety.

New staff (including supply and support staff) will receive information on the school's E-Safety and IT Acceptable Use Policy as part of their induction. All teaching staff will receive regular information and training on e-safety issues in the form of INSET training, and made aware of their individual responsibilities relating to the safeguarding of children in the context of e-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms, including following the school's E-Safety Policy. These behaviours are summarised in this policy which all account holders must read and accept before they can access the school network. When children use school computers, staff must make sure children are fully aware of the agreement they are making to follow the School's IT guidelines.

Staff must check content of material before using it in teaching and be conscious of the age appropriateness of material in relation to the intended audience. Published age ratings on video content must be observed at all times.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They must know what to do in the event of misuse of technology by any member of the school community.

Particular attention will be given to 'gaming' activities using the internet. It is known that this can be a source of inappropriate material for children and provides opportunities for people to 'groom' vulnerable children.

Use of devices in School

Staff

School devices assigned to a member of staff as part of their role must have a password/number so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Staff are permitted to bring personal devices into school but use is restricted in accordance with this policy

Pupils

All pupils are expected to be able to use a desktop/laptop for academic work and guidance is given annually as to the minimum specification considered acceptable for use in school. Advice is also given on security and virus protection and the network scans all devices to ensure they are up to date before allowing connection.

No mobile phones belonging to pupils are to be used during lessons at school without the express consent of the teacher concerned. Pupils are not permitted to walk around the site using handheld mobile devices.

Visitors

This policy also applies to school visitors.

Use of internet and e-mail

Staff

Staff must not access social networking sites, personal emails or any website which is unconnected with schoolwork or business whilst teaching.

Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position.

There is strong anti-virus and firewall protection on the school network and, as such, it may be regarded as safe and secure. Staff should be aware that email communications are monitored. Copies of all emails are retained for future reference should they be needed.

The school will block any website or internet service that it deems to be unsuitable. Any continuing attempts to access an inappropriate site will be reported to the DSL.

Staff must immediately report to a member of the SLT receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring Esland School into disrepute;
- breach confidentiality;

- breach copyright;
- breach data protection legislation;

- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- using social media to bully another individual; or
- posting links or material which is discriminatory or offensive. Under no circumstances should pupils be added as social network 'friends'.

It is recognised that the school is a close and friendly community and that staff may encounter parents and past pupils/parents on an increasing variety of 'networking platforms'. It is the responsibility of staff to ensure where possible that privacy settings are set to prevent any accidental forwarding of postings ('likes' etc) to current pupils. Staff should be mindful that all use of such platforms carry a professional risk and that the points above apply to personal postings should they be read by someone connected in anyway with the School.

Any digital communication between staff and pupils or parents/guardians must be professional in tone and content.

Pupils

There is strong anti-virus and firewall protection on our network called SmoothWall. Spam emails and certain attachments will be blocked automatically by the email system. Furthermore, certain websites are automatically blocked by the school's filtering system. If this causes problems for school work/research purposes, pupils should contact the Headteacher for assistance.

Pupils should immediately report to any member of staff the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Links to both the CEOP and anti-bullying services are permanently on the standard school desktop and available to pupils.

Pupils must report any accidental access to materials of a violent or sexual nature directly to a member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its wi-fi network is monitored.

Password security

Pupils and staff have individual school network logins and storage folders on the server/cloud. Staff and pupils are regularly reminded of the need for password security.

Pupils and members of staff should:

- not write passwords down and should change them regularly (suggest once every 6 months).
- not share passwords with other pupils or staff.

Data Storage

The School takes its compliance with the Data Protection Act 2018 seriously. Please refer to the acceptable use requirements and appendices below for further details.

Staff and pupils are normally expected to save all data relating to their work to the school's cloud.

If staff use personal devices they should be encrypted if any pupil data or school passwords are stored on them. The school expects all removable media USB memory sticks, CDs, portable drives containing pupil data which are being sent by post or courier to be encrypted before sending. Staff may only take information offsite when it is necessary and required in order to fulfil their role.

Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/guardians and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils 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 (eg on social networking sites).

Staff and volunteers are allowed to take digital/video images to support educational aims and for marketing purposes, but must follow this policy concerning the sharing, distribution and publication of those images. On joining the school, parents give their consent for images of their child to be used in this regard.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images.

In accordance with guidance from the Information Commissioner's Office, parents/ guardians are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act).

Complaints

Please see Complaints Procedure

Acceptable use and Appendices

Advice for Parents and Carers - Be Safe and Smart Online

- Talk to your child about what they are up to online
- Keep up-to-date with your child's development online
- Set boundaries in the online world just as you would in the real world
- Encourage the use of complex passwords - eight characters, with a mix of upper and lower case letters and symbols
- Keep technology in the public part of the house
- Ensure safety settings are utilised in all forms of technologies, xBox, phones, pc etc
- Keep virus protection and software up to date
- Engage in their world - don't be a stranger to it!

Additional E-Safety Advice

The links and pdf downloads below provide comprehensive information about online safety .

- ThinkUknow - advice for parents and carers
- CEOP Command Safety Centre - advice for children, parents and carers
- ParentPort - sets and enforces standards across the media to protect children from inappropriate material
- Digizen - information for educators, parents, carers, and young people
- Childnet - a non-profit organisation working with others to help make the internet a great and safe place for children
- BBC Top Ten Online Safety Tips - suggestions to help make sure you don't share too much information online
- KidSMART - online safety advice for children, parents and teachers
- Chat danger - a site all about the potential dangers of interactive services online like chat, IM, online games, email and on mobiles
- Get Safe Online - Free online security advice
- NSPCC Internet Safety - leading children's charity fighting to end child abuse in the UK and Channel Islands
- ChildLine online and mobile safety - tips for staying safe on websites and phones
- O2 - Keeping kids safe - Guide to keeping your family safe in the digital world
- UK Safer Internet Centre - e-safety tips, advice and resources to help children and young people stay safe on the internet
- Net Aware - Guide to online social networks

Esland School Pupil/ Home ICT Acceptable Usage Agreement ICT Acceptable Usage

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices, files and digital communications.
- I will keep my usernames and passwords safe and secure. I will not share them, nor will I try to use any other person's username and password. I will use secure passwords, which include capital letters and numbers. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger" when I am communicating online.
- I will not arrange to meet people offline that I have communicated with on-line, without an adult being aware of the communication and person's motivation for meeting me.
- I will not disclose or share personal information about myself or others when online without an adult's knowledge. (This includes full name, address, email address, telephone numbers, age, gender, educational details, financial details etc.)
- I will not upload images of myself onto any social networking sites.
- I will immediately report any online unpleasant or inappropriate, material or messages, or anything that makes me feel uncomfortable and I am unable to deal with it. I understand this report would be confidential and will help to protect other students and myself.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use, unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act towards me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not behave in a way that can cause damage to ICT systems, and will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download illegal copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school.

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples could be cyber-bullying, use of images or personal information).
- I understand that if I attempt to download copyright material on the school system, the school can track the illegal downloads to me and would then take action against me.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet; temporary or permanent ban on ICT use; detentions; suspensions; contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Esland School Pupil ICT Acceptable Usage Agreement

Name of Pupil

_____

Pupil Signature

_____

Date

_____

Parent/Carer (Home manager) Name

_____

Signature _____

Date _____