Stoneferry Primary School
e-Safety Safeguarding Policy

Date Policy Reviewed: September 2019
Date of next review: September 2020

e-Safety Coordinator/ Deputy Designated Safeguarding Lead/ ICT Co-ordinator – Mr J Boyton
Network manager – RM
Designated Safeguarding Lead – Mr J Boyton
Safeguarding Governor – Mrs L Gadd

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. Stoneferry Primary School endeavours to highlight the benefits and risks of using technology and provides safeguarding and education for users to enable them to control their online experience.

Links to other policies and national guidance
The following school policies and procedures should also be referred to:

- Child Protection Policy
- Whistleblowing Policy
- Behaviour Policy
- Guidance on Safer Working Practice
- Anti-bullying Policy
- Staff code of conduct

The following local/national guidance should also be read in conjunction with this policy:

- Hull Safeguarding Children Partnership, Guidelines and Procedures
- PREVENT Strategy HM Government
- Keeping Children Safe in Education DfE September 2019
- Working Together to Safeguard Children HM March 2018
- Learning Together to be Safe: A Toolkit to help Schools contribute to the Prevention of Violent Extremism

Introduction
The internet has many valuable teaching resources, many of which are available for free. As a school, staff are expected to alert each other to good sites that help to aid teaching and provide excellent learning opportunities children.

Stoneferry Primary School is committed to the safeguarding and welfare of pupils in its care. Children should be kept safe from:

- maltreatment, neglect, violence and sexual exploitation
- accidental injury and death
- bullying and discrimination
- crime and anti-social behaviour in and out of school

Many of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use IT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that IT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will provide a curriculum/PSHCE curriculum/other lessons which has e-Safety related lessons embedded throughout
- We will celebrate and promote e-Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign and will be displayed throughout the school.
- Staff will model safe and responsible behaviour in their own use of

technology during lessons.

- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age- appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-Bullying Policy.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Staff Training

Our staff receive regular information and training on e-Safety issues, as well as updates as and when new issues arise.

- As part of the induction process all new staff receive information and guidance on the e-Safety Policy, the school's Acceptable Use Policies, e-security and reporting procedures. **Staff must read and sign the AUP, and abide fully with this policy at all times.**
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing ICT Systems and Access

- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- All users will sign an Acceptable Use Agreement provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.
- At Key Stage 1, pupils will access the network using an individual username and a class password, which the teacher supervises.
- At Key Stage 2, pupils will have an individual user account with an appropriate password which will be kept secure, in line with the pupil Acceptable Use Agreement. They will ensure they log out after each session.
- All internet access will be undertaken alongside a member of staff or, if

working independently, a member of staff will supervise at all times.

- Members of staff will access the network using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password, as per the staff AUP.

Managing Filtering

The school has a Netpilot firewall/filtering system as part of the managed service internet provision from KCOM, with ad-hoc amendment by the network manager on request. Banned phrases and websites are identified by the device in real-time from the McAfee Trusted Source Web Database, which include:

- **Discrimination** – Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, culture or sex
- **Drugs/Substance abuse** – displays or promotes the illegal use of drugs or substance
- **Extremism** – promotes terrorism and terrorist ideology, violence or intolerance
- **Malware/Hacking** – promotes the compromising system, including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
- **Pornography** – displays sexual acts or explicit images
- **Piracy and copyright** – includes illegal provision and copyright materials
- **Self-harm** – promotes or displays deliberate self- harm (including suicide & eating disorder)
- **Violence** – displays or promotes the use of physical force intended to hurt or harm

- The school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training/online safety lesson.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Co- ordinator immediately.
- If users discover a website with potentially illegal content, this should be reported immediately to the e-Safety Coordinator. The school will report such incidents to appropriate agencies including the ISP, Police,CEOP or the IWF.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed by the headteacher/e-Safety Coordinator prior to being released or blocked.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Information system security

- Virus protection automatically updates from the central management server which is monitored by the network manager.
- There are 10 wireless points in school.
- IT security will be discussed regularly with the school's network manager.

E-Mail

- All staff will have a school email account which should only be used for school related work.
- Some pupils from year 3 upwards may be issued with a secure school e-mail account through the Its Learning Platform. This will only permit e mails to be sent to registered users on Stoneferry's Its Learning account.
- When pupils leave the school their e-mail account and school access will be ceased.
- When staff cease employment with the school their accounts will closed and access to the network will be stopped.
- The admin account will be checked on a regular basis by the Headteacher for inappropriate content, in her absence this will be done by the IT TA.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain letters is not permitted.

Encryption

- All school devices that hold personal data (as defined by the Data Protection Act 2018) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the Trust's Data Protection Officer to ascertain whether a report needs to be made to the Information Commissioner's Office. *(Note: Encryption does not mean password protected).*

Social Networking

- Staff should not post inappropriate content or participate in any conversations which will be detrimental to the image of the school. Staff who hold an account are advised not have parents as their 'friends'. Staff should not accept current pupils at the school as 'friends', doing so may result in disciplinary action or dismissal.
- School blogs or social media sites should be password protected and run from the school website with approval from the Senior Leadership Team.

Publishing pupil's images and work

- Photographs that include pupils or their work will be selected carefully and will not enable individual pupils to be identified by their full name.
- Pupils' full names will not be used anywhere on the Website or the school's Twitter account, particularly in association with photographs and video.
- Photograph permission forms are signed when pupils start school. These are held by the school.
- Written permission is obtained from parents/carers before photographs and videos are published. Parents sign this agreement on entry and the permission lasts for the length of time their child is at the school, unless they inform us otherwise.
- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- Pupils and staff are not permitted to use their own portable devices to store images/video/sound clips of pupils.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Mobile Phones and Devices General use of personal devices

- Mobile phones and personally-owned devices are not permitted to be use in any way during lessons or school time. They should be switched off or silent at all times.
- No images or videos are permitted to be taken on mobile phones or personally owned devices.
- In the case of school productions, Parents/carers are permitted to take photographs of their own child in accordance with school protocols which strongly advise against the publication of any such photographs on social networking sites.

Pupils' use of personal devices

- Pupils who need to bring a mobile phone into school can only do so if a written request is received from parents explaining the reason that a mobile phone is needed.
- Parents sign an agreement that states that they have discussed the appropriate use of mobile phones with their child. This reinforces the rule that mobile phones will be switched off as soon as the pupil enters the school building and will be taken to the office for safe keeping. They must not be kept in classrooms or cloakrooms.
- Pupils who do not follow the school policy relating to the use of mobile phones will not be permitted to bring their mobile phones into school.

Staff use of personal devices

- Staff are only permitted to use their mobile phones within restricted areas in school. Staff are not permitted to take personal calls or access text messages during session times or when they are on duty. Phones may only be used in personal break times.
- Staff will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

Protecting personal data

- When leaving a PC unattended all staff and pupils in key stage 2 will be asked to lock their workstation until they return. All workstations will lock automatically after two minutes
- Staff are required to keep work laptops and USB sticks in a safe place at all times to avoid them being picked up by another party and information viewed or used by others.
- Staff are only permitted to use encrypted memory sticks in school. These will be provided on loan to all staff by the school.
- When staff leave the school they are expected to remove content from their memory stick and return it to school.
- Children are not permitted to bring in memory sticks from home without prior permission from a member of staff.
- When off the school premises, information viewed is the staff member's responsibility. Staff are advised to be vigilant with who uses the laptop and monitor closely what the laptop is used for.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- The loss of USB memory sticks can lead to serious consequences due to data protection legislation.

CCTV

- The school may use CCTV in some areas of school property as a security measure.
- Cameras will only be used in appropriate areas and there is clear signage indicating where it is in operation.

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy' before using any of school ICT resources.
- All parents will be required to sign the home-school agreement prior to their children being granted internet access within school.
- All visitors and students will be made fully aware of the school's Acceptable Use Policy prior to being given internet access within the school.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.

Support for Parents

- Parents' attention will be drawn to the school's e-Safety policy and safety advice in newsletters, the school website and e-Safety information workshops.
- The school website will be used to provide parents with timely and meaningful information about their children's school lives and work to support the raising of achievement. The website will also provide links to appropriate online-safety websites.

Online sexual harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.
Online sexual harassment, which might include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats.

Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified.

Stoneferry Primary School follows and adheres to the national guidance - UKCCIS: Sexting in schools and colleges: Responding to incidents and safeguarding young people, 2016.

Screening, Searching and Confiscation

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Child Protection/ Designated Safeguarding Leaders). Regular monitoring and filtering is in place to ensure that access to inappropriate material on the internet and key word reporting is in place to ensure safety for all staff and pupils.

Sexting

Someone taking an indecent image of themselves and sending to their friends or boy / girlfriend via a mobile phone or some other form of technology is sometimes referred to as 'Sexting'. Young people need to be aware that they could potentially be distributing illegal child images. Staff working at Stoneferry Primary will ensure that pupils are aware of the risks associated with the use of the internet and how to respond appropriately to a 'Sexting' incident. We know this can cause enormous distress to children and young people and may place them at risk of sexual grooming and other risks associated with the internet.

Response to an Incident of Concern

An important element of e-Safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff, volunteers and pupils have a responsibility to report e-Safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school has incident reporting procedures in place and record any incidents of an e-Safety nature. All e-Safety concerns/ incidents are to be recorded on CPOMs (in the same way any other incident/ concern is logged).

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or expulsion, in accordance with the school's Behaviour or Discipline Policy. The school also reserves the right to report any illegal activities to the appropriate authorities.

Policy Updated: September 2019
Policy Review Date: September 2020 or when changes are necessary to comply with school policy or national legislation.