AVON HOUSE
PREPARATORY SCHOOL

CELEBRATING & SUPPORTING EVERY CHILD

E-Safety Policy
(Technology Security and Electronic Communications)

Introduction

ICT in the 21st Century is seen as an essential resource to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment.

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguarding awareness and awareness for users to enable them to control their online experience.

As computing is an area which undergoes constant change; this document should reflect these developments and the needs and requirements of the children and staff at Avon House School.

Scope

The policy covers all staff and provides guidelines on work equipment and personal equipment, where these are used for work purposes. This policy must be read in conjunction with the School Handbook, the School's social media and Networking Sites Policy, Data Protection Policy and Privacy Notice The policy covers:

- the internet and servers
- all forms of electronic communication – email, social media, etc.
- electronic bulletin boards and social media
- file sharing by whatever means
- computing devices including desktops, laptops, printers, mobile devices, etc.
- communications equipment including telephones, mobiles, video conferencing, etc.

This policy, supported by the Acceptable Use Procedures for staff and pupils, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

At Avon House School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

Roles and responsibilities

The Designated Safeguarding Lead (DSL) and Headteacher have responsibility for ensuring this policy is upheld by all members of staff. They will keep up to date on current e-safety issues and guidance issued by organisations such as the Local Authority, Child Exploitation,

Online Protection (CEOP) Childnet International, the Local Authority Safeguarding Children Board and the Prevent Duty guidance. As with all issues of safety at the School, staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis and this includes an awareness of material pupils may access on the internet. The statutory guidance makes clear the need for the School to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. The school has suitable filtering in place monitored by London Grid for Learning (LGfL). The School has an important role to play in equipping pupils to stay safe online, both in school and outside. Internet safety is integral to the School's ICT curriculum and is embedded in the ICT and RPS curricula. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website:
http://www.saferinternet.org.uk

Raising awareness

*"**All** staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/ misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content."* **KCSIE**

New members of teaching staff receive this E-Safety Policy and Acceptable Use Procedures as part of their induction. All teaching staff receive information and training on e-safety issues in the form of INSET training, internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All staff who supervise children using ICT complete an online e-safety assessment annually, through the school's online providers Educare and National Online Safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-safety procedures and summarised within the Acceptable Use Procedures. These procedures are shared with the children and reinforced during computing sessions throughout the academic Year. 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 will know what to do in the event of misuse of technology by any member of the School community. Any concerns must be recorded by staff as soon as possible within the blue incident and concern books after any safeguarding incident relating to e-safety occurs and be given directly to the School's DSL.

Creating a curriculum and culture of E-Safety

ICT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and monitor and assess our pupils' understanding of it. The School provides opportunities to teach about e-safety within a range of curriculum areas and ICT lessons. Educating pupils on the dangers of technologies that

may be encountered outside school will also be carried out via RPS, as well as informally when opportunities arise. At age-appropriate levels, and usually via ICT and RPS, pupils are taught to look after their own online safety. Pupils are taught in the RPS curriculum about recognising safeguarding threats online, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL or any member of staff at the school. From Year 3, pupils are also taught about relevant laws applicable to using the internet. Pupils are taught about respecting other people's information and images etc. through discussion and classroom activities. Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see Anti-bullying Policy). Pupils should approach the class teacher as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies. In an effort to make this area of the curriculum more accessible for the pupils, the introduction of 'Be Internet Legends' developed by Parent Zone and Google. This also offers internet safety curriculum resources for Key Stage 2 pupils. To promote this area further the school has also purchased access to 'The National Online Safety' website. Through this platform the school hopes not only to develop the structure of how online safety is taught but also to be more impactful in how it engages with parents, initially starting with engagement through the school newsletter 'the weekly flight' highlighting computing issues and offering guidance in the form of how to deal with emerging key computing issues.

Use of school and personal devices

Devices assigned to a member of staff as part of their role and must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff must ensure that it is locked to prevent unauthorised access. Staff at the school are permitted to bring in mobile phones for their own use, however, they are not permitted to connect to the school network. Staff are not allowed to have their phone switched on during the working day, unless they are in the school staffroom or School Office. Personal telephone numbers may not be shared with pupils and under no circumstances may staff contact a pupil using a personal telephone number.

Pupils

Mobile technologies available for pupils are generally not permitted unless it is an aid to learning any items fulfilling these criteria are stored in locked cupboards.

Year 6 children are permitted to bring in mobile phones to ensure that they may be contacted by parents whilst travelling to and from school; the devices are collected at registration and sent to the school office where they are kept in a locked cupboard and the children collect their devices from the school office in readiness for journeys home.

Pupils should be aware that all ICT use, including email communications can be monitored. This E-Safety policy and the Acceptable Use Procedures apply to all pupil and staff personal devices in school.

All pupils in Years 3-6 are issued with their own personal Google school e-mail addresses. Access is via a personal login, which is password protected. Pupils should be aware that

email communications are monitored. Senso.cloud is employed by the school as a way of monitoring all managed Chromebook devices offering keystroke recognition and tracking.

There is strong anti-virus and firewall protection on our network. Spam emails, certain websites and certain attachments should be blocked automatically by the email system. 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. Pupils must report any accidental access to materials of a violent or sexual nature directly to any member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be 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.

Remote or online working

There may be times or occasions when pupils may need to work online or remotely. The school has set out a system for the pupils to use Google Classroom for such times or circumstances. The pupils will have received training in the safe use of this portal and the expectations we have as they work. Part of the portal is for communication. Whilst we would advocate only using this for communication with school staff for pastoral or academic support or in a supervised discussion group, we are aware that the system does allow for pupils to communicate with other peers when the teacher is not present or online. Pupils will be reminded that conversations should not take place on matters other than school related and that if the school finds conversation trails that are inappropriate in nature the pupil will face behavioural sanctions. 'Hangouts' will be treated in the same way as a face to face conversation. We do not tolerate conversations of a derogatory nature including racial, gender, ethic, unkind or inequality comments and would treat any such conversations or posts as serious. The class teacher will refer these to a senior member of staff. In a period of lockdown where we cannot put some sanctions in place due to the closure of on-site working, the SLT will put in place a sanction that they feel is appropriate at the time. Pupils who need to use the internet for research should restrict their search to the topic they are working on and not stray from the subject. Should behaviours be deemed unacceptable the parent of the child will be contacted immediately. (Cross referenced to the school Behaviour and Discipline Policy)

Data storage

The School takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy and the Acceptable Use Procedures for further details.

Password security

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

Employees must:

- use unique passwords and PIN; password details must be logged with the school's ICT support – Stuart Macleod (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers)
- Change passwords routinely and at any indication of a system compromise
- Be aware of their individual responsibilities to protect the security and confidentiality of the school network

Managing filtering

- The school employs LGFL as its main filtering provider, using keystroke recognition software to track any misuse
- The school will work with the local authority and the internet service provider to ensure systems to protect pupils are reviewed and improved
- If pupils or staff discover an unsuitable site, it must be reported to the class teacher, ICT teacher or the school's ICT support
- The school's ICT support will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before its use in school is allowed
- The use of portable media such as memory sticks will be monitored closely as potential sources of computer virus and inappropriate material and the school has provided each member of staff with an encrypted USB stick
- Pupils are not generally allowed to bring personal mobile devices/phones to school. Any phones that are brought to school will be sent to the school office and kept there until the end of the day
- Staff will use a school phone where contact with a parent is required; and a school mobile if contact is necessary whilst offsite

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

The school cannot accept liability for the material accessed or any consequences of internet access. The school will audit ICT provision to establish if the E-Safety Policy is adequate and that its implementation is effective.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where the consent could be an issue

- Parents/carers may withdraw permission in writing at any time
- Photographs that include pupils will be selected carefully
- Pupils' full names will not be issued anywhere on the school website, particularly in association with photographs
- Pupils' work can only be published by outside agencies with the permission of the pupil and parents

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs and video footage taken are for private retention and not for publication in any manner and when appropriate will ask that no footage of any kind be taken.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by the Head Teacher
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the DSL and will be recorded in the Incident and Concern books.
- Any complaint about staff misuse must be referred to the Head Teacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Pupils and parents will be informed of the complaint's procedure

Virtual Learning Environment (VLE)

The school's VLE is run through Google Classroom. Each pupil (from Foundation 1 to Year 6) has a user account and can view work set by teachers online. Pupils' work is stored on their Google drive and teachers review and feedback to the pupils. Online records tracking pupils' interactions and work log can be used to feedback to parents and inform teachers' decisions for tracking and progress.

Pupils' Email

The Google mail system for the pupils and teachers is a closed system. This means that communication can only occur between addresses with the same domain i.e. @avonhouseschool.co.uk. By using emails in this manner, the school has limited the idea of outside influence whilst maintaining the pupils' access to technology and online experiences.

Policy Violations

Any violations or suspected violations must be reported immediately. Any non-compliance with the above policy will be dealt with through the school's disciplinary policy.

CELEBRATING & SUPPORTING EVERY CHILD

Reviewed December 2018 GB
Reviewed August 2019 GB/NH
Reviewed August 2020 GB/AC
Reviewed April 2021 GB
Reviewed August 2022 GB/NH
Reviewed February 2023 GB/NH