Stanbridge Lower School

E-SAFETY POLICY

Internet Safety and Internet Security

Reviewed: June 2018

1. AIMS/RATIONALE

1.1 At Stanbridge we feel that rapidly developing information and communication technologies (ICT) are exciting and motivating learning tools through which learning and teaching can be greatly enhanced.

1.2 We feel that ICT is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

1.3 The staff and governors at Stanbridge also believe that keeping children safe and teaching children about e-safety is essential. We need to ensure that ICT is used safely and responsibly and that risks related to ICT use are properly managed.

1.4 Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The World Wide Web
- E-mail
- Instant messaging often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites .
- Video broadcasting sites .
- Chat rooms .
- Gaming sites .
- Music download sites .
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications
- On-line learning resources.

The staff and governors at Stanbridge feel they have a duty to ensure that children have a working understanding of how to keep themselves safe whilst using these applications and work towards developing this understanding when using the internet in school.

1.5 E-Safety procedures address all safeguarding issues which relate to the use of ICT. There are two main elements to these issues

- E-Security: procedures to ensure all electronic data is categorised as public, restricted or protected and that electronic systems containing data are securely maintained.

- E-Safety: procedures to ensure all members of the school community know their access rights and responsibilities in using ICT. These procedures are expressed in our school's Acceptable Use Policy (AUP)

1.5 The procedures and elements of this policy support BECTA guidelines and OFSTED safeguarding requirements.

2. RESPONSIBILITIES

2.1 E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head and Subject Leader, with the support of Governors, aims to embed safe practices into the culture of the school.

2.2 The responsibility for E-Safety has been designated to Rosemary Godwin (Head Teacher) who is the designated person for Child Protection. The E-Safety Co-ordinator will work closely with and delegate tasks to Mrs Nita Coupland (ICT Support).

2.3 Our E-Safety and ICT Subject Leader ensures they keep up to date with E-Safety issues and guidance through liaison with the Local Authority E-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP). The school's E-Safety Subject Leader ensures the Head, senior management and Governors are updated as necessary.

2.4 All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. Central to this is fostering a 'No Blame' culture so students feel able to report any bullying, abuse or inappropriate materials.

2.5 All staff should be familiar with the school's policy including:

- Safe use of e-mail
- Safe use of Internet including use of internet-based communications services, such as instant messaging and social networking.
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile 'phones and digital cameras
- Publication of student information/photographs and use of website
- E-Bullying/Cyber bullying procedures
- Their role in providing E-Safety education for students.
- Staff are reminded/updated about E-Safety matters at least once a year.
- Compliance with the General Data Protection Regulations 2018

2.6 The E Safety and ICT Subject Leader will review the E Safety Risk Assessment and GDPR Policy annually and report any recommendations to the Governing Body.

2.7 Information Classification: The following restrictions apply to all information in school and staff have a duty to follow these guidelines

Restricted Information Containing Sensitive Personal Data	Protected Information	Public Information
Personal information related to pupils and staff contained in all Management Information Systems eg Integris, Classroom Monitor etc. Examples of these are SEN information, reports, academic results, medical information etc.	School routines, schedules and management information	Website and promotional materials, display material around school, school dates etc
Should only be accessed by the Head Teacher and staff with designated passwords. Teaching/Office Staff: should only transfer restricted data using an mobile device with permission of Head Teacher, or use ofAnycomms. All transfer of paper records should be signed for	Can be accessed by all staff on the shared curriculum area. This is password protected.	Accessed by all via websites

2.8 All mobile storage devices are vulnerable to theft or loss and there are confidentiality risks when using these away from school. ***Staff should not store any restricted information/data on mobile storage devices.***

2.9 The Head Teacher will keep a log of all mobile devices used and who they are allocated to. Staff should not use their own mobile devices in school eg laptops, ipads, external drives. All mobile devices should be owned and issued by school.

2.10 Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office

2.11 All staff shall take responsibility for their own use of technologies, taking appropriate steps to ensure they use technology safely, responsibly and legally. Inappropriate use exposes Stanbridge Lower School to risks including virus attacks, compromise of network systems and services, legal issues and pupil safety.

2.12 Staff should be aware that all school ICT activity and on-line communications may be monitored, including any personal and private communications made via the school network.

2.13 All members of staff with access to ICT systems shall be responsible for taking the appropriate steps to select and secure their passwords. These steps should include:

- Keeping passwords secure from pupils, family members, and other staff
- Using a different password for accessing school systems to that used for personal (non-school) purposes
- Choosing a password that is difficult to guess or difficult for pupils to obtain by watching staff log in.
- Adding numbers or special characters (eg !@£$%^)
- Changing passwords regularly eg each term
- Staff should not write their passwords down unless absolutely necessary and then in a location that cannot be accessed by anyone else.
- When leaving a computer for any length of time, all staff shall log off or lock the computer, using CTRL+ATL+DELETE

.

3. MANAGING THE INTERNET SAFELY

3.1 Pupils will

- Be taught what Internet use is acceptable and what is not and given clear training in Internet use
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Take part in Internet Safety Day annually raising the awareness of how to be safe and responsible users of technology and what to do if they are bullied, made to feel uncomfortable or abused online.

3.2 Teachers will

- Fosters a 'No Blame' environment which encourages staff to tell a teacher/responsible adult immediately if they encounter any material which makes them feel uncomfortable.
- Ensures students know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or E-Safety Co-ordinator.
- Ensures students are taught how to evaluate Internet content and to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Ensures students and staff know what to do if a cyber bullying or other E-Safety incident occurs.

3.3 The Co-ordinator will

- Ensures staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or E-Safety Co-ordinator. Refer to the *What To Do If...?* and fill out the *E-Safety Incident Form#*
- Ensure the school Internet access will include filtering appropriate to the age of students
- Ensure virus protection is installed on all computers used for internet access
- Ensure any unsuitable material inadvertently discovered on the internet by a school user must be reported to the Head Teacher straightaway, who will inform
- The Co-ordinator will then inform the ISP to block future access to that site.

4. AUTHORISING INTERNET ACCESS

4.1 All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource

4.2 The school will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdrawn

4.3 Throughout the school students' access to the Internet will be through adult demonstration with occasional directly supervised access to specific, approved online materials

4.4 Parents will be asked to sign and return the *E-Safety Agreement Form*

4.5 All students must read and sign the *Rules for Responsible ICT Use* before using any school ICT resource

4.6 Teachers will have access to student e-mails and related internet files for monitoring and assessment.

5. INTERNET AND DATA SECURITY

5.1 We prevent the exploitation of technical vulnerabilities bysing the latest versions of operating systems, web browsers, applications ensuring these are updated regularly. Filtering system blocks sites which fall into categories such as pornography, race hatred, gaming, sites of an illegal nature; and which informs staff and students that they must report any failure of the filtering systems directly to the teacher.

5.2 We have a well configured firewall as this is recognised as the first line of defence against external attack and can help prevent data breaches by blocking malware and hacking attempts.

5.3 Insight;our ICT technicians company manage this for us.

6. E-SAFETY: E-MAILING

6.1 Students:

- We only XXXXXXX with students
- Students should only use the XXXXX school domain e-mail accounts on the school system
- Students are introduced to, and use e-mail as part of the ICT scheme of work and given guidance on safe and acceptable use and reporting procedures
- Students have their own logins and passwords and students must keep their logins and passwords secret
- In addition to the above points, students must still refer to the *Rules for Responsible ICT Use.*
- Make it clear that students should never be allowed to logon or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network
-

6.2 Staff:

- Staff can use the XXXXX/school domain e-mail accounts or web-based e-mails for professional purposes or for legitimate personal uses deemed 'reasonable' by the Head and Governing Body

- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff should change their passwords at regular intervals
-
- Staff are responsible for the content of all outgoing and incoming e-mail and will ensure acceptability of the content; and will handle any inappropriate material they receive in such a way as to help protect the school's ICT resources and shield others form harmful or offensive material
- Spam is unavoidable and issues about spam should be referred to the ICT Manager/E-Safety Co-ordinator straightaway. That person can inform people how to direct spam through a spam filter and will contact the ISP for further advice.
- Foster a 'No Blame' environment which encourages staff to tell a teacher/responsible adult immediately if they encounter any material which makes them feel uncomfortable.
- For the safety of both staff and pupils it is not acceptable for staff to e-mail pupils, except through the Learning Platform when in connection with the pupil's learning. Eg comments about homework. ***This statement relates to an employment tribunal decision:***

  Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging or telephone. Should special circumstances arise where such communication is felt to be necessary, the agreement of a line manager should be sought first and appropriate professional language should always be used

7. MOBILE PHONES

There is a clear expectation that all personal use of mobile phones is limited to allocated lunch and/or tea breaks and must be used off the premises or in the staffroom. **Mobile phones should not be used in classrooms or any other area of the school and must be locked away in lockers or lockable drawers.**

7.1 Staff are not permitted to use their own personal phones for contacting children, young people and their families within or outside of the setting when working with children in their professional role. **No personal data relating to parents and children eg telephone numbers, addresses should be stored on personal phones.**

7.2 Members of the school staff may take photographs on mobile phones in special circumstances with the permission of the Head Teacher and in the presence of another member of staff. Photographs must be downloaded and wiped from the phone before the member of staff leaves the school building. Images of pupils will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent/ carer. Staff may only take photographs of children who's parent's have given permission for their child to be photographed.

7.3 Any individual bringing a personal device into the setting must ensure that it contains no inappropriate or illegal content.

7.4 Driving: If any practitioner is required to drive in a working capacity, and has responsibility for the work mobile, the phone must be switched off whilst driving. It is strongly recommend that practitioners follow the same procedures regarding their own personal mobile phones. Under no circumstances should practitioners drive whilst taking a phone call. This also applies to hands-free and wireless connections, which are considered a distraction rather than a safer alternative.

7.5 **Children** are not permitted to have their phone about their person on school premises or on school visits.

7.6 **Parents, visitors and contractors** are respectfully requested not to use their mobile phones in any area where children are present. Should phone calls and/or texts need to be taken or made, this should be done off of school premises.

7.7 Any individual bringing a personal device into the setting must ensure that it contains no inappropriate or illegal content.

7.8 School/ Work Mobile: The use of a designated work mobile is promoted as it is:

- an essential part of the emergency toolkit which is taken on off-site trips.
- an effective communication aid, enabling text, email messages and calls to be made and received.

7.9 We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school

7.10 Staff are not allowed to use photographic or video devices in changing rooms or toilets.

8. DIGITAL IMAGES AND VIDEO AND VOICE RECORDING

8.1 Staff may use allocated school devices such as IPads and class cameras to take photographs/recordings of children for curriculum, teaching and learning, observations, displays etc where their parents have given permission for us to do so.

8.2 All images should be stored on the curriculum area. We do not use students' names when saving images in the file names.

8.3 We do not include the full names of students in the credits of any video materials/DVDs produced and published by the school.

9. E-SAFETY: USING THE SCHOOL NETWORK EQUIPMENT AND DATA

9.1 At Stanbridge

- Staff read and sign that they have understood the school's E-Safety Policy. Following this, they are set-up with internet and email access and can be given an individual network login username and password
- It is clear that no-one should logon as another user.
- We ensure that each student and staff member has their own My Documents and is responsible for maintaining their own files
- We require all users to always log off or lock computers when they have finished working or are leaving the computer unattended
- Where a user finds a logged on machine, we require them to always log off and then log on again as themselves and report this to the ICT Subject Leader as a breach in security.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs. Staff must read and sign the *ICT Equipment Loan Scheme Agreement.* All laptops loaned to them by the school should not be used by other family members or persons. If this is done, it is done so at the risk of the person to whom the laptop is on loan to.

10. THE SCHOOL WEBSITE

10.1 Website photographs that include images of pupils will be selected carefully and will not enable individual pupils to be clearly identified by their name. We will only use images of children whose parents have given us permission to do so.

10.2 Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

10.3 The Head Teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

10.4 Photographs found on our school website are view only and cannot be downloaded or copied.

11. DISPOSAL OF RECORDS

11.1 Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we override electronic files. We may at times also use an outside company to safely dispose of electronic records.

11.2 We routinely "weed" electronic data and paper based records that are no longer relevant or out of date.

12. TRAINING

12.1 Our staff and governors are provided with E-safety and data protection training as part of their induction process. All staff and governors are briefed on their

responsibilities for the creation, use, maintenance and eventual destruction of records. They are briefed on security as set down in this policy.

12.2 Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

13. INFRINGEMENTS AND POSSIBLE SANCTIONS.

13.1 How will infringements be handled?: When a student or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the Head Teacher. The following are provided as exemplification only:

Students

1. **Category A infringements**
   - Use of non-educational sites during lessons
   - Unauthorised use of email
   - Use of unauthorised instant messaging/social networking sites
   - ***(Possible sanctions: referred to class teacher /E-Safety Co-ordinator)***

2. **Category B infringements:**
   - Continued use of non-educational sites during lessons after being warned
   - Continued unauthorised use of email after being warned
   - Continued use of unauthorised instant messaging/chatrooms, social networking sites, News Groups
   - Corrupting or destroying others' data without notifying a member of staff of it
   - Accidentally accessing offensive material and not logging off or notifying a member of staff of it.
   - ***(Possible sanctions: referred to class teacher/E-Safety Co-ordinator/senior teacher/removal of Internet access rights for a period /contact with parent).***

3. **Category C infringement:**
   - Deliberately corrupting or destroying someone's data, violating privacy of others
   - Sending an email or MSN message that is regarded as offensive, harassment or of a bullying nature (one-off)
   - Deliberately trying to access offensive or pornographic material
   - Any purchasing or ordering of items over the Internet
   - Transmission of commercial or advertising material
   - ***(Possible Sanctions: referred to Class teacher/E-Safety Co-ordinator/Head Teacher/removal of Internet and/or Learning Platform access rights for a period/contact with parents/removal of equipment).***

4. **Category D infringements:**
   - Continued sending of emails or MSN messages regarded as offensive, harassment or of a bullying nature after being warned
   - Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
   - Use or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
   - Bringing the school name into disrepute.
   - ***(Possible Sanctions – referred to Head Teacher/Contact with parents/possible exclusion/removal of equipment/refer to Community Police Office/LA E-Safety Co-ordinator).***

Staff

Category A infringement (Misconduct)

- Excessive use of internet for personal activities not related to professional development eg online shopping, personal email, instant messaging etc
- Misuse of first level data security eg wrongful use of passwords
- Breaching copyright or license eg installing unlicensed software on network
- Acting in an unprofessional manner on social networking sites eg Facebook to gossip about, bully, abuse or insult others in the school community.
- To publish school information, photographs or other similar material on social networking sites without permission from the Head Teacher.
- ***(Sanction – referred to line E Safety Co-ord/Head Teacher/warning given).***

Category B (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school/Council computer hardware or software
- Any deliberate attempt to breach data protection or computer security rules
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Use or transmission of material which infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute
- ***(Sanction – referred to Headteacher/Governors and follow school disciplinary procedures; report to AL Personnel/Human Resources, report to Police)***

13.2 E Safety - safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop and preserve any evidence

- Instigate an audit of all ICT equipment by an outside agency such as the school's ICT managed service providers – to ensure there is no risk of students accessing inappropriate materials in the school
- Identify the precise details of the material.
- If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.
- Schools are likely to involve external support agencies as part of these investigations eg an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

14. CHILD PORNOGRAPHY FOUND

14.1 In the case of child pornography being found, the member of staff should be **immediately suspended** and the Police should be called.

14.2 Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection Centre (CEOP): http://www.ceop.gov.uk/reporting abuse.html

15.INCIDENT REPORTING

15.1 It is the responsibility of all staff to report breaches to the E-Safety / ICT Subject Leader so that they can be dealt with effectively and in a timely manner in order to minimise any impact on school.

15.2 The E-Safety Subject Leader will maintain an Incident Log. This log shall capture the following information: Incident date, description of occurrence, immediate corrective action, further action, legal implications, closed date.

15.3 The Incident Log will be reviewed by the Head Teacher once per term and the risk assessment shall be updated in light of new incidents. The Head Teacher will review the Risk Assessment and any accompanying Action Plans with the Curriculum Sub Committee annually.

15.4 Procedures for report abusive content on social media sites can be found attached to the policy. These are published by NAHT and are called Appendix 2: Procedures for Reporting Abusive Content on Social Media Sites. It is strongly recommended that a screenshot is taken before removing offensive material from sites. The screen shot should be taken in the presence of a colleague and the whole process documented eg signed and dated by more than one person. Please see Appendix 1 to ensure screenshots are handed sensitively and comply with the first data protection principle.

16.REVIEW OF POLICY

The school's policy will be reviewed when:

- Annually alongside the GDPR, Child Protection Policy.

- There has been a significant change in staffing or pupil intake.
- There has been a significant change in Government guidelines

.

R GODWIN
HEAD TEACHER
June 2018

This policy was ratified by the full governing body.

Date of Meeting: ……..

Signed …… Chair of Governors.

Appendix 1

Handling Screenshots

Handling screenshots must comply with the first data protection principle set out below…

In practice it means that you must

- Have legitimate grounds for collecting and using the personal data
- Not use the data in ways that have unjustified adverse effects on the individuals concerned
- Be transparent about how you intend to use the data and give individuals appropriate privacy notices when collecting their personal data
- Handle people's personal data only in ways they would reasonably expect
- Make sure you do not do anything unlawful with the data

(taken from the Information Commissioners Officer)