Eagle House School (Sutton)
Online Safety Policy

1. INTRODUCTION

This policy is also applicable to Eagle House 6th Form (Strawberry Lodge) which is registered as part of the main school in Sutton.

The 'Working Together to Safeguard Children' March 2015 and 'Keeping Children Safe in Education' July 2015 documents set out how organisations and individuals should work together to safeguard and promote the welfare of children. The revised guidance planned for 5th September 2016 will be used to update this policy.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for

Many of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. 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.

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online safety Policy, as part of the wider safeguarding agenda, outlines the approach taken to help ensure our pupils are prepared to deal with the safety challenges that the use of technology brings.

The Online safety Policy relates to other policies including those for Safeguarding and Promoting the Welfare of Children, ICT and Anti-Bullying.

The Designated Safeguarding Personnel at Eagle House School (Sutton) are:

- Designated Safeguarding Lead: Martyna Sobczak-Roberts
- Deputy Designated Safeguarding Lead: Ruth Duggan, Deputy Head – 6th Form
- Deputy Designated Safeguarding Lead: Yvonne Gordon, Pupil Wellbeing Officer

2. TEACHING AND LEARNING

Why the Internet and digital communications are important

The school has a duty to provide pupils with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. ICT will be used across the school to enhance and extend learning, to engage in interesting and vibrant learning activities and to empower learners so that they play a more active role in managing their own learning experiences.

Internet use will enhance learning

The school's Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils will be taught the importance of cross-checking information before accepting its accuracy.

3. MANAGING INFORMATION SYSTEMS

Information system security

School ICT systems security will be reviewed regularly. Virus protection will be updated regularly.

Each commissioning Local Authority will be provided with this policy.

Email

Pupils are not permitted to send emails at school, unless this is part of a planned programme of study which forms part of the curriculum and is fully supervised by staff.

Published content and the school website

The contact details given on the website will be the school address, e-mail and telephone number. Staff or pupil personal contact information will not be published.

The Schools' Business Office in liaison with the Business Development Manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil images and work

Written permission should be sought from parent/carers before photographs of pupils are published on the school website.

Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.

Parents/carers should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

Social Network sites and newsgroups are not allowed to be accessed at the school.

Pupils and parents/carers will be advised that the use of social network spaces outside school brings a range of dangers for children and young people. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Managing filtering

The school will work with appropriate agencies and partners to ensure systems to protect pupils are reviewed and improved.

If staff or pupils come across unsuitable on-line materials, the site must be reported to the Head of Education and action taken to ensure it cannot be accessed again.

Senior staff will ensure that regular checks are made by the schools IT support provider to ensure that the filtering methods selected are appropriate, effective and reasonable.

Monitoring procedures

The school will undertake the monitoring of school devices used by staff and pupils on a regular basis. This may include the monitoring of emails, jpegs and internet browse histories.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Staff mobile phones and similar devices are only permitted to be used for non-work purposes outside of lesson time, in the Staff Room or where agreed in advance with the Head of Education. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

Pupils are strongly discouraged from bring their mobile phones, tablets or similar devices to school. If a pupil brings one to school, for instance because they have been using it to play games during a long taxi journey to school, they will place in in their bag up on arrival and will not be allowed to access it during the school day. Or pupils may hand their phone in to be stored in an individual phone locker at reception for safe keeping and collect it at the end of the day. If a pupil attempts to use a mobile device during the school day it must be taken to Reception to be securely locked away and collected at the end of the school day. Appropriate tuition in the social use of devices for texting and snapchat, for example, will be provided on a need-to-know basis through the PSHE and SRE curriculum.

The school uses photographs and videos as a key tool to record pupil progress and each class has its own camera. Staff are not permitted to take the camera home with them. Staff are not allowed to use their own personal devices to take photographs or videos of children. Should a situation arise where this is deemed necessary, for instance the class camera breaks, the member of staff must seek permission for SLT before doing so and the device used must not be taken off the school site until all such photographs /videos have been removed from it.

Similarly staff are not permitted to take any of the schools mobile phones home and pupils are not permitted to use school mobile phones to take photographs

Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Pupils are not allowed to use these devices for accessing the internet.

The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Visitors are not permitted to use their phones to take videos or photographs whilst on site.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the requirements of the Data Protection Act 1998.

4. POLICY DECISIONS

Authorising Internet Access

All staff must read and sign the Acceptable Use Policy for ICT before using any school ICT resource.

All pupils (or their parents/carers if more appropriate) must read and sign the Acceptable Use Policy for ICT before using any school ICT resource.

Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources before being allowed to access the internet from the school site.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material, including providing appropriate close supervision. However, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

The school will monitor the use of ICT to establish if the Online safety policy is adequate, appropriate and effective.

Handling Online safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Senior Leadership Team.

Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures.

Pupils and parents/carers should be informed of the complaints procedure.

Pupils and parents/carers will be informed of consequences for pupils misusing the Internet. This may include the loss of internet privileges.

5. COMMUNICATIONS POLICY

Introducing the Online safety policy to pupils

Online safety rules will be displayed in the ICT suite and discussed with pupils regularly.

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

A programme of training in Online safety will be developed with frequent updates for all staff (and pupils where appropriate).

Online safety awareness will be embedded within the Computing scheme of work and the PSHE curriculum to support pupils to develop an understanding of how to stay safe on line.

Staff and the Online safety policy

All staff will be given access to the School Online safety Policy and its importance will be explained.

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff will always use a child friendly, safe search engine when accessing the web with pupils. Filters are in place for search engines such as *Google*.

To maintain appropriate boundaries, staff are not permitted to befriend pupils on social network spaces. This also applies to past pupils who, due to their social communication difficulties, may still have misconceptions and misunderstandings about the boundaries of social network 'friendships', despite their older age.

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School Online safety Policy in newsletters, the school brochure and on the school website. Where a pupil is unable to understand and sign the Acceptable Use Policy, parents/carers will be asked to sign it so show they understand the expectations the school has of pupils in relation to Online safety.

The school will maintain a list of Online safety resources for parents/carers.

6. POLICY REVIEW

It is the responsibility of the Head of Education supported by the other members of the school's Senior Leadership Team to monitor this policy. It should be reviewed annually or when new legislation is published.

7. RELATED POLICIES AND DOCUMENTATION

- Safeguarding and Promoting the Welfare of Children Policy

- ICT Policy
- Anti-Bullying Policy
- Data Protection Policy

Appendices:-

- *Acceptable Use Policy: Permanent and Temporary Staff*
- *Acceptable Use Policy: Pupil*

Document:	Online Safety Policy
Date adopted/written:	September 2012
Last Reviewed:	January 2018
Next review:	January 2020
Version:	Final

ICT Acceptable Use Policy for Staff

Guidelines for all permanent and temporary staff using the Internet and ICT at School.

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head of Education. Please read and agree to the following.

☐ I will only use the school's email/internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head of Education.

☐ 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 ensure that all electronic communications with pupils and staff are compatible with my professional role, this includes not befriending parents/carers or pupils on social networking sites, such as *Facebook* and not emailing pupils. This includes all past pupils.

☐ I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils or parents/carers. Maintaining contact with former pupils for purposes of transition support and school monitoring should be done through the teacher's school email account and only with the prior permission of the Head of Education.

☐ I will only use the approved, secure e-mail system(s) for any school business.

☐ I will ensure that personal pupil data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head of Education. Personal or sensitive data taken off site must be encrypted.

☐ I will not install any hardware or software without the permission of the system administrator.

☐ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory or could otherwise cause embarrassment or risk for the school.

☐ Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent from the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer/member of staff and Head of Education.

☐ I will ensure that any photos taken of pupils do not compromise their dignity, wellbeing & safety

☐ I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset or offend any member of the school community.

☐ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head of Education.

☐ I will respect copyright and intellectual property rights.

☐ I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.

☐ I will support and promote the school's Online safety and Data Protection policies and help pupils to be safe and responsible in their use of ICT and related technologies.

☐ I will immediately inform the Head of Education of any actual or suspected breach of these guidelines I become aware of.

☐ I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature: ..... **Date:** .....

Full Name: ..... (PRINTED)

PASSWORDS

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords on paper or in an unprotected file
- Only disclose your personal password to authorised ICT staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Passwords must contain a minimum of six characters including a mix of lower and upper case letters, numbers and a symbol, and be difficult to guess
- User ID and passwords for staff and pupils who leave the School are removed from the system within 3 months
- If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

The school may exercise the right to monitor the use of the school's computer system, including access to web-sites, the interception of email and the deletion of inappropriate materials where it

believes unauthorised use of the school's computers system is or may be taking place, or the system is or may be used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

ICT Acceptable Use Policy for Pupils

These rules help us to be fair to others and keep everyone safe. Please read each rule below carefully and agree to them.

☐ I will endeavor to leave my mobile phone, ipad or tablet at home.

☐ If I do bring my mobile phone, ipad or tablet to school, on arrival I will place it in my bag and leave it there at all times, I will not use it or attempt to use it during lesson time, including times when I am moving from one classroom to another. Alternatively I will lock my mobile phone or iPad or tablet in a secure locker in the office when I arrive at school in the morning. I will collect it before I leave for home at the end of the day.

☐ I understand that if I try to use my mobile phone during lesson time it will be confiscated and placed in a secure locker in Reception . I will be able to collect my phone before I leave for home at the end of the day

☐ I will only log onto the computers with my own username and password.

☐ I will not tell others outside the ICT support team my password.

☐ I will only open my own files and shared files.

☐ I will only delete my own files.

☐ I will not install any software onto the school's computers.

☐ I will ask permission before using the internet.

☐ I will never give out the personal details of myself or others (for example, name, address, phone numbers, etc.)

☐ I will not use chat sites.

☐ I will not use social networking sites such as Facebook and Twitter.

☐ I will only e-mail people I know, or people my teacher has approved.

☐ The messages I send will be polite and sensitive.

☐ I will ask for permission before opening an email or an email attachment sent by someone I don't know.

☐ If I see or receive anything that is offensive or that makes me feel uncomfortable I will tell a member of staff immediately.

☐ I will not attempt to bypass the school's internet filtering system.

☐ I will not publish any picture taken of any pupil at Eagle House School unless permission has been given.

☐ I understand that the school may check my computer files and the internet sites I visit.

☐ I will take responsibility for my behaviour when using the internet.

☐ I understand that if I deliberately break these rules, I may not be allowed to use the internet or computers.

The school may exercise the right to monitor the use of the school's computer system, including access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's computers system is or may be taking place, or the system is or may be used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Eagle House School (Sutton)
ICT Acceptable Use Agreement

I (the pupil) have read and agree to all of the rules above for the acceptable use of ICT at Eagle House School (Sutton).

Signature: ..... **Date:** .....

Full Name: ..... (PRINTED)

I (the parent/carer) have read and agree to all of the rules above for the acceptable use of ICT at Eagle House School (Sutton).

Signature: ..... **Date:** .....

Full Name: ..... (PRINTED)

Parent/Carer can sign on the pupil's behalf to acknowledge understanding of the Online safety expectations for their child at Eagle House School (Sutton).