Hughenden Primary School
ICT and Social Media Policy

Policy statement:

Safeguarding is a serious matter; at Hughenden Primary we use technology and the internet extensively across all areas of our curriculum. Online safeguarding, known as e-safety, is an area that is constantly evolving and as such is this policy will be reviewed on an annual basis or in response to a serious e-safety incident, whichever is sooner.

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents - any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School: - any school business or activity conducted on or off the school site, e.g. visits, conference, school trips etc.

Wider school community - all students, all staff, governing body, parents and partner school.

Third Party Provider – an authorised ICT specialist service provider appointed by the school.

Encryption – converts information or data into a code to prevent unauthorised access.

The primary purposes of this policy are to:

1. Ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.

2. Ensure risks are identified, assured and mitigated (where ever possible) in order to reduce any foreseeability of harm to the student or liability to the school.

A copy of this policy and School Home agreement are distributed to parents upon first entry to the school. Upon return of the signed Home school agreement, which will be taken an acceptance of the school’s term and conditions, children will be allowed to use school technology and use the internet.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to the Designated Safeguarding Leads and/or Team as indicated below.

Hughenden Primary School will ensure that:

- E-safety training throughout the school is planned and up to date and appropriate to the recipient, i.e.: students, all staff, senior leadership team and governing body, parents.
- The Designated and Deputy Designated Lead for Safeguarding has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

The Safeguarding Team will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review policies regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, SLT and the governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for logging e-safety incidents, ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measure in school (e.g.: internet filtering software, behaviour management software0 are fit for purpose through liaison with the local authority and/or ICT technical support.
- Make themselves aware of any reporting function with technical e-safety measure, i.e.: internet filtering reporting functions; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff (Third Party Provider)

Technical support staff are responsible for ensuring that the IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devise.
- Operating system updates are regularly monitored and devices updates as appropriate.
- Any e-safety technical solutions such as internet filtering are operating correctly.

- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Designated Person for Child Protection and Headteacher.
- Passwords are applied correctly to all users regardless of age.
- The IT System Administrator password is to be changed on a minimum of a ½ termly basis or at notification of a breach; whichever is the sooner.
- Password protection of all laptops, tables and desktop computers.
- Encryption of all files that contain sensitive or other restricted information.

All Staff

Staff are to ensure that:

- All details within this policy are personally understood. If anything is not understood it should be brought to the attention of the DSL
- Any e-safety incident is reported to the DSL or a member of the Safeguarding Team. If you are unsure the matter is to be raised with the safeguarding team to make a decision.

Pupils

The boundaries of use of computing equipment and services in this school are given in the Home School Agreement and the Internet Code of Practice. Deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour for learning policy.

E-safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all pupils will be fully aware how they can report areas of concern whilst at school or outside school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will work with parents to enhance the skills and knowledge they need to protect children outside the school environment.

Through parents evenings, school newsletters and email communication the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that pupils are empowered.

Parents must also understand the school needs to have in place to ensure that their child can be properly safeguarded. As such, parents need to sign the pupil Internet Code of Practice before access can be granted to school ICT equipment or services.

Technology

Hughenden Primary School use a range of devices including PC's, laptops and tablets in order to safeguard the pupil and in order to prevent loss of personal data. We employ the following assistive technology:

- **Internet Filtering** – The local authority operates filtering software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Third Party Provider and the Safeguarding Team are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher or DSL as appropriate.
- **Email Filtering** – Email filtering is in place that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e.: malware) that could be damaging or destructive to data; spam email such as a phishing message.
- **Encryption –** All school devises that hold personal data, as defined by GDPR are encrypted. No data about the school is to be on an un-encrypted devise; all devises 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 key drives is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local to ascertain whether a report needs to be made to the ICO. **Note:** encryption does not mean password protected. All laptops have a bit locker code.
- **Passwords** – all staff and pupils will be unable to access any device without a unique username and password. Staff passwords are strong and robust and are changed if there has been a compromise. The Third Party Provider will be responsible for ensure that passwords are changed. Any terminals not in use must be logged off or the screen must be locked to prevent misuse**.**
- **Anti-virus** – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. The Third Party Provider will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

Safe Use

- **Internet** – Use of the internet in school is a privilege, not a right, Internet use will be granted to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.
- **Emails –** All staff are reminded that emails are subject to Freedom of Information requests and SCR's (Subject Access Requests) and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted. Students are permitted to use the school email system and as such will be given their own email address.
- **Photos and videos –** Digital media such as photos and videos are covered in the schools' Home School Agreement. All parents must sign a photo/video release slip at

the beginning of each academic year; non- return of the permission slip will not be assumed as acceptance. Any photos or film taken on any device must only be stored on OneDrive/ Shared drive – not left on it.

- **Social Networking -** A Broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be “followed” or “friended” on these services and such no two-way communication will take place.
- **Child Identity -** Permission slips (via the Home School Agreement) must be consulted before any images or video of any child is uploaded and there is to be no identification of students using first name and surname; first name only is to be used.
- **Copyright law -** 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 licence that allows for such use (i.e. creative commons)
- **Notice and take down policy –** should it come to the schools attention that there is a resource that has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.
- **Incidents –** Any e-safety incident is to be brought to the immediate attention of the Safeguarding Team, or in their absence, to the Headteacher. The Safeguarding Tam will take the appropriate action to deal with the incident and will fill out an incident log.
- **Training and Curriculum –** It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Hughenden will have an annual program of training provided to students, staff, parents and carers.
- **Training -** As well as the programme of training, we will establish further training or lessons as necessary in response to any incidents. All staff, and visiting trainees, must have system specific training as well as e-safety training via the IT support.
- **Child E-Safety -** E-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student’s learning.
- **E-Safety Officer** - The E-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and Safeguarding Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training and/or experience in any particular area, this must be brought to the attention of the SLT for further consideration.

Appendix A: Acceptable Use Policy

Use of Hughenden School ICT resources is granted based on acceptance of the following specific responsibilities:

Software

Only licenced software may be installed onto school laptops & computers. Software currently installed on the computer includes the following: Microsoft Explorer, Outlook Suite and 365.

Teachers are not authorised to install unlicensed software on computers. If a teacher requires special or non-standard software to be installed on computers for school use, it must be cleared by the Network Manager beforehand. The teacher will be responsible for supplying licences, media, and any documentation. Licence information is a requirement for the County Auditors.

Software in use in the School is licenced in a correct and legal manner. However (except where explicitly stated), it is not available to users for home usage. Users should make no attempt to copy licenced or copyrighted material from the school network.

Users may not download copyrighted software, audio or video files, or any other copyrighted material from the Internet. Any such material found will be deleted without prior notification and may result in disciplinary action.

Breach of these conditions may lead to disciplinary action.

Networking

For network connection of computers, users are provided with a dedicated account. The user is to use no other account on the network. The user should at all times keep any passwords for this account secure and private. The user takes full responsibility for the use and misuse of this account.

This account allows the user certain privileges and rights on the network. The user should in no way attempt to gain other privileges to attempt to access resources on the network to which no explicit rights have been granted.

The user shall not in any way, tamper or misuse school equipment, either software or hardware. No form of tampering is acceptable.

Computers can have access to the Internet. Abuse of this access, in the form of access to pornographic sites is absolutely forbidden. Please note that access to certain pornographic sites may be in serious breach of the law (Child Trafficking and Pornography Act 1998). The school will fully co-operate with the relevant authorities in investigating and prosecuting any such illegal access.

General:
The facilities are for School related educational use only. The facilities are not available for use on external projects or for work activities not associated directly with the courses or the School. Facilities may not be used for any form of personal financial gain.

The contents of all mailboxes, PCs, server shares and caches operated by the School, remain the property of the School. The status of these data stores is similar to that of letters posted to the School to a post holder (not marked as personal and private).

Email should be considered as an insecure medium for the transmission of confidential information. Where confidential information is to be transferred, in particular externally, it should be done so in an encrypted from. Notwithstanding that every effort is made to ensure that home folders and e-mails are secure, the School does not in any way guarantee the security of this data.

Social Networking

We understand that social networking sites and blogging are extremely popular. Users must not post material which damages the reputation of the school or which causes concern about their suitability to work with children and young people. Those who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct.

Basic Security

Protect the access and integrity of computing and information technology resources. For example: it is a violation to release a virus or worm that damages or harms a system or network to prevent others from accessing an authorised service to send email bombs that may cause problems and disrupt service for other users to attempt to deliberately degrade perform or deny service to corrupt or misuse information to alter or destroy information without authorisation.

General usage

Food and drinks should be kept well away from computers. The user should also take care when shutting down and closing the lid of laptops to ensure that nothing is left lying on top of the laptop surface. This may result in damage not covered by warranties, in which case the user will be liable for repair costs.

Authorisation

Use only those computing and information technology resources for which you have authorisation. For example: It is a violation; to use resources you have not been specifically authorised to use, to use someone else’s account and password or share your account and password with someone else to access files, data or processes without authorisation to purposely look for or exploit security flaws to gain system or data access.

Intended use

Use computing and information technology resources only for their intended purpose. For example: it is a violation to send forged email to misuse networking, Internet Relay Chat (IRC)

Instant Messaging software to allow users to hide their identity, or to interfere with other systems or use electronic resources for harassment or stalking other individuals to send bomb threats or “hoax messages” to send chain letters to intercept or monitor any network communications not intended for you to use computing or network resources for advertising or other commercial purposes to attempt to circumvent security mechanisms.

Law

Abide by applicable laws and school policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software. For example, it is a violation to make more copies of licenced software than the licence allows to download, use or distribute pirated software to operate or participate in pyramid schemes to distribute pornography to minors to upload, download, distribute or possess child pornography.

Privacy

Respect the privacy and personal rights of others. For example: it is a violation to tap a phone line or run a network sniffer without authorisation to access or attempt to access another individual’s password or data without explicit authorisation to access or copy another user’s electronic mail, data, programs or other files without permission.

This policy was approved by the Governing Body on 2nd July 2018.

It is due to be reviewed on 2nd July 2021.