



HOWE GREEN HOUSE SCHOOL

eSafety Policy

Based on the Hertfordshire model for eSafety

ISI Reference	2a
Issue Number	1
This policy is endorsed by	Governing Body and the Head
This policy is owned by	Senior Deputy Head
Review Body	Education Committee

Most Recent Revision Date	September 2021
Last Reviewed by Governors	May 2021
Period of Review	Every 2 years
Next Review Date	May 2023
Previous Reviews	May 2021

To be made available	YES
To be on website	YES
Internal staff only	NO
Internal students only	NO
Internal staff and students	YES

Contents

Introduction	4
Roles and Responsibilities.....	5
eSafety skills development for staff.....	5
Managing the school eSafety messages	5
eSafety in the Curriculum	6
Data Security	8
Infrastructure	9
Managing other Web 2 technologies.....	10
Mobile technologies.....	11
Personal Mobile devices (including phones)	11
School provided Mobile devices (including phones)	11
Acceptable use and conditions of using school provided mobile devices	11
Managing email.....	13
Safe Use of Images	14
Taking of Images and Film.....	14
Consent of adults who work at the school	14
Publishing pupil’s images and work.....	14
PUBLISHING A PUPIL’S IMAGE ONLINE	14
Storage of Images	15
Video Conferencing.....	15
Misuse and Infringements	16
Complaints	16
Inappropriate material.....	16
Equal Opportunities	17
Students with additional needs	17
Parental Involvement.....	18
Writing and Reviewing this Policy.....	19
Staff involvement in policy creation	19
Review Procedure	19
ICT Acceptable Use Agreement: Staff	20
Smile and Stay Safe Poster.....	22
Howe Green House School code of conduct for remote learning – 09/03/21 v3.....	23
Current Legislation.....	26
Acts relating to monitoring of staff email.....	26
Data Protection Act 1998.....	26
Regulation of Investigatory Powers Act 2000.....	26
Human Rights Act 1998.....	26
Other Acts relating to eSafety.....	26
Racial and Religious Hatred Act 2006	26
Sexual Offences Act 2003.....	26
Communications Act 2003 (section 127).....	26
The Computer Misuse Act 1990 (sections 1 – 3)	26
Malicious Communications Act 1988 (section 1).....	27
Copyright, Design and Patents Act 1988.....	27
Public Order Act 1986 (sections 17 – 29).....	27
Protection of Children Act 1978 (Section 1)	27
Obscene Publications Act 1959 and 1964.....	27
Protection from Harassment Act 1997	27

Our eSafety Policy has been written by the school, building on the Hertfordshire Grid for Learning exemplar policy.

INTRODUCTION

ICT in the 21st Century is seen as an essential resource to support learning and teaching, 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 young people with the skills to access life-long learning and employment.

Information and Communications Technology 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. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Twitter
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Howe Green House School, we understand the responsibility to educate our students on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

ROLES AND RESPONSIBILITIES

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in our school is Mr Martin who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts / Essex LA, ISA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

eSafety is discussed at the weekly SLT meetings under the category of Safeguarding. eSafety is reported to the Governing body under the category of Safeguarding.

This policy, supported by the school's acceptable use agreements for staff and the code of conduct for remote learning (for staff, parents and children) is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PHSE.

ESAFETY SKILLS DEVELOPMENT FOR STAFF

- Our staff receive information on eSafety issues in the form of emails, relevant training. Updates in staff meetings etc.
- New staff receive information on the school's eSafety policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community
- Our staff, governors and visitors (if appropriate) all agree to an AUP
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas as appropriate.
- All staff receive eSafety training – this may be discrete training or as a part of the ongoing safeguarding training.

MANAGING THE SCHOOL ESAFETY MESSAGES

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- E-safety is taught to the students at the start of each school year as part of the IT curriculum and is also taught in the relevant PHSE units.

ESAFETY IN THE CURRICULUM

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the students on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching eSafety as part of the PSHE programme.
- The school has a framework for teaching internet skills and eSafety in ICT lessons
- Educating students on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them (as appropriate to the age of the child).
- Students are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities (as appropriate to the age of the child).
- Students are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

PASSWORD SECURITY

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All staff read and agree to an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Our staff agree to an AUP
- Staff and students are provided with an Office 365 account and login details. They are also provided with a network account and access to educational resources such as Purple Mash.
- If students forget their login details or think another person knows their password then they can ask their Form Tutor for help in the first instance. Depending on the platform, the teacher will be either be able to reset the password or will be able to contact the school IT support to request that this happens.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and CPOMS, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked or that they have signed out.

DATA SECURITY

The accessing and appropriate use of school data is something that the school takes very seriously.

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the person's role.
- To comply with the Data Protection Act all pupil data is stored and accessed within the school's network. To access the network a password is required. Most data is stored in Engage which is password protected, although some data is stored in external databases for assessments (GL assessments) and educational learning platforms such as Purple Mash.
- Any data taken off the school premises must be stored on a secure removable device (i.e. a device which is password protected)

MANAGING THE INTERNET

The internet is an open communication medium, available to all. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whilst on site, the children are always supervised when accessing the internet.

- The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites and resources before use.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

INFRASTRUCTURE

- School internet access is controlled through our web filtering service which is provided by and monitored by Herts IT Services.
- Howe Green House School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Students are aware that school based email, Teams and internet activity can be monitored and explored further if required.
- If staff discover an unsuitable site, the web page must be noted and then closed and the incident reported immediately to the e-safety co-ordinator.
- If students discover an unsuitable site, the laptop screen should be folded shut (or monitor switched off) and the incident reported immediately to the teacher. The teacher will then note the details of the web page and will report the incident immediately to the e-safety co-ordinator. The web page will be closed by the teacher who will check that the laptop is safe and ready to return to the student.
- Anti-Virus protection is provided by and updated by Herts IT Services
- Students' parents and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems
- Students are not permitted to download or upload programs on school based technologies.
- If there are any issues related to viruses or anti-virus software, the IT Co-ordinator should be informed. The IT Co-ordinator will liaise with IT support. In the absence of the IT Co-ordinator, IT support at BIT Solutions should be contacted directly and the IT Co-ordinator should be copied in to any communication via email.

MANAGING OTHER WEB 2 TECHNOLOGIES

Web 2 (the read/ write internet), including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking sites to students within school.
- The current age limit for creating a social media account is 13. Therefore, the school does not expect that any children would have one. It does recognise that there are parents who will allow this and so children are educated in the appropriate use of and dangers related to social media.
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our students are asked to report any incidents of bullying to the school.
- Staff are only permitted to communicate with children electronically through the child's school email account, Teams and Purple Mash. Such communication has been necessitated by Covid 19 and the need to provide remote education and to communicate with children electronically.
- Staff should be aware of information that they are putting into the public domain (Facebook, Myspace, Twitter, YouTube etc). Staff should not allow children or young people to be listed as their "friends" and should not allow themselves to be listed as "friend" on students' sites.
- Staff may only communicate with parents electronically through their school email accounts, Teams or via Zoom.

MOBILE TECHNOLOGIES

Many emerging technologies offer new opportunities for teaching and learning with laptops more readily used in classrooms. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

PERSONAL MOBILE DEVICES (INCLUDING PHONES)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- Staff must ensure that all personal digital devices that are used to access school data, such as email and SIMs have appropriate security enabled.
- Staff mobile devices are to be stored securely, out of reach of children.
- Staff should not use personal mobile devices whilst children are in the same room.
- If a student does need to bring a mobile device into school then this will be handed to the form tutor who will keep it safe and return it at the end of the school day.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages or posting of inappropriate comments between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

SCHOOL PROVIDED MOBILE DEVICES (INCLUDING PHONES)

- The sending of inappropriate text messages or posting of inappropriate comments between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.

ACCEPTABLE USE AND CONDITIONS OF USING SCHOOL PROVIDED MOBILE DEVICES

Where possible, all teaching staff are provided with a laptop with access to appropriate systems. The school IT Services (BIT Solutions) will create usernames and passwords for new staff and the school office will provide this information once a member of staff commences employment. Tablets may also be provided depending on availability.

No software should be loaded without the authority of the IT Co-ordinator. Once this has been obtained staff should ask the IT Manager to load the software. Applications downloaded on tablets must be for school use only. Teaching staff who are given tablets may download school related applications using their own Apple account and will be reimbursed accordingly.

The laptops and tablets may be required to be brought into school for inspection or updating at any time.

Laptops and tablets may be used by pupils **only** when supervised by staff.

When not in use laptops and tablets must be stored securely and not left in open view out of normal working hours.

These laptops and tablets remain the property and responsibility of Howe Green House School (HGHS) and must not be used by family members or other parties outside the staff of HGHS, nor should they be used for any purpose other than related school business. In addition staff should not store any data on the laptop or tablet which they would consider personal to them, as all data stored on HGHS equipment is assumed to be the property of HGHS and therefore subject to review at any time by the HGHS IT Co-ordinator or any member of the senior leadership team.

Information must not be backed up on any cloud based servers with the exception of those officially sanctioned by the SLT e.g. for use with Tapestry, school Office 365 accounts. Photographs should be regularly uploaded from any portable devices to the school network and then deleted from the device.

Please remember that your network password is your insurance that no-one else can access your account and you are therefore responsible for ensuring that your password is not disclosed to any other person. If you believe that your personal password has been compromised then you should change it immediately and inform the IT Co-ordinator.

Should any inappropriate material be found on any laptop or tablet then this may result in disciplinary measures, and should any illegal material be found then the appropriate authorities will be informed.

Any data stored on the device must not be used for any purpose other for legitimate and sanctioned school use. Inappropriate use of such data may result in disciplinary measures, and should any activity be considered illegal then the appropriate authorities will be informed.

Should you have any problems with your laptop or tablet then please advise the BIT Solutions and copy in the IT Coordinator.

By accepting responsibility for a mobile device (using it on or off site), a member of staff is accepting the terms and conditions stated in this policy.

MANAGING EMAIL

The use of email within most schools is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects within school or international.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact students, parents or conduct any school business using any personal communication methods, e.g. non-school email address, Whatsapp, social networking, twitter, video sites etc.
- Parents and pupils must only attempt to communicate with staff via their school email accounts, in writing, via the school telephone number or in person.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending sensitive emails to external organisations, parents or students are, in the first instance, advised to send a draft version to their line manager / relevant members of the SLT if they think the issue might be contentious. Once the wording has been agreed, they are advised to cc or bcc in their line manager / relevant members of the SLT.
- Staff are expected to check their email regularly throughout the day and to respond to any queries from parents or other staff within 24 hours – a holding email is perfectly acceptable in the first instance particularly if action or investigation is needed.
- Staff are not expected to check work emails after 5.00 pm and before 8 am during weekdays or during weekends.
- During school holidays staff are only expected to check work emails by the final Friday before a return to school
- If parents need to contact the school during school holidays then they will be directed to use the main school email address.
- If the school urgently needs to contact a member of staff they will do so by telephone.
- Students may only use the Office 365 email accounts provided by the school.
- The forwarding of chain letters is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive e-mail.
- Students are introduced to email as part of the ICT Scheme of Work.

SAFE USE OF IMAGES

TAKING OF IMAGES AND FILM

Digital images are easy to capture, reproduce and publish and, therefore, misused.

- Parents or carers must opt out if they do not want appropriate images of their child to be used within the school or on the web site or school social media platforms or for promotional material.
- Students must not take or distribute any inappropriate images/ audio/ video of members of the school community.

CONSENT OF ADULTS WHO WORK AT THE SCHOOL

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

PUBLISHING PUPIL'S IMAGES AND WORK

On a child's entry to the school, all parents/guardians will be asked to opt out if they do not wish their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
- On the school's social media platforms

This consent is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be withdrawn an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time.

E-mail and postal addresses of students will not be published.

PUBLISHING A PUPIL'S IMAGE ONLINE

Parents and teachers must not upload any images / videos onto the internet of any children other than their own which have been taken during any school events (this includes **all** online platforms including social media). If a parent wishes to post an image of their child then the image must be cropped to exclude any other children.

STORAGE OF IMAGES

- Images/ films of children are stored on the school's network and the web site
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network.

VIDEO CONFERENCING

- Parents can opt out of allowing their children to participate in video conferencing.
- When in school, all students are supervised by a member of staff when video conferencing
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked. Therefore staff will be present during any video conferences delivered by external speakers.

MISUSE AND INFRINGEMENTS

COMPLAINTS

Complaints relating to eSafety should follow the school complaints procedure unless they are Safeguarding issues in which case they will adhere to the safeguarding policy. Complaints will be recorded in the correct log as appropriate with the incident itself (complaint / bullying / safeguarding). Details will also be recorded on CPOMs as appropriate.

INAPPROPRIATE MATERIAL

- All users are aware of the procedures for reporting accidental access to inappropriate materials.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the member of staff on CPOMs, depending on the seriousness of the offence; investigation by the Headmaster/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences. Staff are made aware of sanctions relating to the misuse or misconduct by having an Acceptable Use Agreement which they agree to every time they login.
- The schools discipline procedures will be used for all ICT / eSafety offences.

EQUAL OPPORTUNITIES

STUDENTS WITH ADDITIONAL NEEDS

The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

PARENTAL INVOLVEMENT

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and students are actively encouraged to contribute to adjustments or reviews of the school eSafety policy by placing the policy and AUA on the school website and asking for feedback.
- Parents/ carers are required to make a decision as to whether they wish to remove their consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
 - Website
 - Newsletter items
 - Talks by guest speakers

WRITING AND REVIEWING THIS POLICY

STAFF INVOLVEMENT IN POLICY CREATION

- Staff have been involved in making/ reviewing the eSafety policy through circulation to all staff for comments and feedback.

REVIEW PROCEDURE

- There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them
- This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning.
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.
- This policy has been read, amended and approved by the staff, head teacher and governors on

ICT ACCEPTABLE USE AGREEMENT: STAFF

ICT and the related technologies such as email, 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 Ian Martin, school eSafety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- 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 students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, social networking username, twitter account and personal email address, to students or parents unless sanctioned by the Headteacher. Nor will I use any of the above for personal communication with students or parents unless sanctioned by the Headteacher.
- I will not follow or be followed by children or existing parents on any social media platform – this includes being in any Whatsapp group. The only exception is if you are a parent of a child at Howe Green House and a member of staff and it is necessary to communicate regarding non-school business e.g. to arrange children's parties etc. All communication relating to your role as an employee of the school must still take place using your school email account / in writing / using a school phone.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on Engage) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data taken offsite should only be done using an encrypted portal device.
- I will not install any hardware or software without permission of the Network Manager or eSafety Coordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional purposes in line with school policy.
- 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 Headteacher.
- I will respect copyright and intellectual property rights.
- I will not bring into school any illegal content, including pirated songs, movies, software, offensive material and will not try and share or distribute it further.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute. This will include for example, posts on social networking sites, video and photo publishing and sharing sites.
- If remote learning is required then I will comply with the code of conduct for remote learning
- I will support and promote the school's e-Safety policy and help students to be safe and responsible in their use of ICT and related technologies.

User agreement (by staff)

By using ICT in school and off site I agree to follow this code of conduct and to support the safe use of ICT throughout the school and understand that it is a condition of being employed at the school.

ICT ACCEPTABLE USE AGREEMENT: STUDENTS

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc. for school purposes.
- If I discover an unsuitable site, I will switch the screen off and immediately tell my teacher.
- I will not invite any member of the school staff to become “a friend” on social networking or similar types of sites.
- I will not download or install software on school technologies.
- I will only log on to the school network/ Learning Platform (e.g. My Maths, Purple Mash) with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone.
- If I need to communicate with a teacher by email, I will only use my school email address or my parent will communicate on my behalf.
- I will make sure that all digital communications with students, teachers or others is responsible, appropriate, inoffensive and sensible. This is both inside and outside of school and includes all electronic communication such as texting, chat messages through Teams etc. If I feel bullied online then I know that it is important to tell my parent/ carer or a teacher and do not suffer in silence. I also know that there are sites such as Childline/ CEOP where I can get further help.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I must seek permission from my teacher before I take, store and distribute images, audio or videos of students and/ or staff. These digital recordings must never be of an inappropriate or offensive nature. If asked to delete any digital recordings I will do so from all media (i.e. USB, home computer etc)
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring it into disrepute.
- I will respect the privacy and ownership of others’ work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies will be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer or even the police may be contacted.
- I will not bypass or attempt to bypass any of the security features provided at the school.
- I will not bring into school any illegal content, including pirated songs, movies, software, offensive material and will not try and share or distribute it further.
- I will change my password if I think someone else knows it.
- I understand that the school does not approve of any children having social media accounts e.g. Tik Tok, Snapchat, Facebook, Instagram, You tube. These sites require children to be 13 years old to hold an account.

User agreement (by parents on behalf of their children)

By using ICT in school and off site I agree to follow this code of conduct and to support the safe use of ICT throughout the school and understand that breaches may lead to disciplinary measures.

SMILE AND STAY SAFE POSTER



Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

HOWE GREEN HOUSE SCHOOL CODE OF CONDUCT FOR REMOTE LEARNING – 09/03/21 V3

Statement of intent

To enable the school to provide children with meaningful education during a time of prolonged school closure and to continue to educate children who are self-isolating following Government guidance on Covid, the school is committed to providing remote learning throughout the normal term times.

This provision will take place using a combination of approaches as determined by the individual teacher meaning that children are able to continue to learn using printed resources and instruction as well as teacher interaction through online platforms.

In order to provide remote learning using online platforms it is essential that all members of the school community behave in a responsible manner: the expectations of behaviour and conduct applied in school also apply online. Therefore, by signing in to the Office 365 account that the school has provided you are signing up to the code of conduct detailed below. This code of conduct is aimed at parents who will be responsible for their child's account and online conduct; the code of conduct also applies to members of staff employed by Howe Green House School .

The Office 365 suite including Teams has been provided for school use. If parents allow children to communicate with each other electronically then it should not be conducted using the school accounts. It is the decision and responsibility of a parent allow a child to communicate electronically and as such they are expected to monitor this and to deal with any consequences.

The School policy for safety underpins this code of conduct. This policy is available on request to the school office.

For parents who would like to find out more about how to help keep their children safe online and to help encourage children to become responsible digital citizens, please click on the link below:

<https://www.saferinternet.org.uk/advice-centre/parents-and-carers>

Rules and conditions for accessing and providing remote learning at Howe Green House School

Account and Login details

- Your username and password are unique to you and must not be shared with other students.
- You are responsible for any communication that is sent from your account.
- The school retains the right to monitor and access all school Office 365 accounts.
- The school retains the right to delete an account if the code of conduct is breached severely and / or repeatedly.

Communication

- Office 365 will act as the only form of communication between the child and staff. No personal accounts or alternative applications must be used with the exception of school sanctioned learning platforms such as MyMaths and Purple Mash. Zoom may be used by staff instead of Teams to conduct lessons and Reception will also use Tapestry.
- Staff and parents will continue to communicate with each other in the same way that they currently do electronically which is by using the official school email addresses – if in any doubt parents should send a message to the main school email address which will be forwarded as appropriate. No attempt should be made to contact staff or parents via the online video chat function within office 365.
- Staff and parents must be mindful of and are responsible for the appropriate use of, tone and content of any electronic communication.
- Parents are expected to monitor their child's electronic communication in the same way as they would be expected to do so already if they have permitted their child to communicate this way previously.
- If inappropriate messages are sent using the school office 365 accounts then a screen shot should be taken and an email should be sent to the Form Tutor with an accompanying email explaining the issue in the first instance.
- Parents and children must not attempt to use Teams to video / audio call members of staff outside of the core teaching day.

Troubleshooting

- If your child is unable to access Office 365 or any of its applications then please email the school in the first instance.
- Please copy your child's Form Tutor into this email
- If your child is unable to access a resource or link sent by a teacher then please contact that teacher and let them know – they may be able to solve the issue or it may be necessary for us to contact our IT support.

Safeguarding:

- If you have any safeguarding concerns then please contact Mrs Mills and copy Mr Martin and Mrs McNally in on the email.
- The school's current safeguarding policy is available on the school website should you need to refer to it.

Hours of operation

- Remote learning will run in line with the timetable provided.
- Staff will be expected to check their emails regularly throughout the day from Monday to Friday between 8 am and 5 pm and to respond within 24 hours.
- Children and parents should not expect staff to communicate with them outside of these hours.

Video conferencing

- Teams and Zoom will be used to live stream lessons where appropriate. There is the same expectation with regards to behaviour during these sessions as there would be in an actual class based lesson.
- Children should mute their microphone during explanations. Repeated unnecessary interruptions may lead to the removal of the child from the remote lesson.
- All participants must be fully clothed during video conferencing sessions.
- Children and parents are not permitted to record the sessions without express permission from the teacher running the session.
- Should any recording be permitted then this must not be shared with any 3rd parties or posted anywhere else on the internet.
- If instructed to disable the camera function to allow audio chat only, then children must do so.
- Parents should not interrupt lessons. Please refer to the section on communication with regards to how to contact staff.

We reserve the right to amend these rules and conditions over time. Should this be the case then parents will be emailed a revised version by the School.

CURRENT LEGISLATION

ACTS RELATING TO MONITORING OF STAFF EMAIL

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

<http://www.hmsso.gov.uk/acts/acts1998/19980029.htm>

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

<http://www.hmsso.gov.uk/si/si2000/20002699.htm>

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

<http://www.hmsso.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998

<http://www.hmsso.gov.uk/acts/acts1998/19980042.htm>

OTHER ACTS RELATING TO ESafety

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

For more information

www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.