GIGGLESWICK SCHOOL
E-SAFETY POLICY

Introduction

It is the duty of Giggleswick School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

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

- Safeguarding Policy and Procedures
- Staff Code of Conduct for Contact with Students;
- Health and Safety;
- Behaviour & Exclusions; GJS Behaviour Policy
- Anti-Bullying; GJS Anti-Bullying Policy
- Acceptable Use Policy;
- Data Protection;
- Bring Your Own Device (for staff and students);
- Curriculum for Life; GJS PSHCEe Policy;
- Mill-House Mobile Devices Policy; and
- Mobile Device Usage Policy

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online 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 Giggleswick School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas**.**

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.
Both this policy and the Acceptable Use Policy (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

Roles and responsibilities

1. The Governing Body
The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually, with regular scrutiny from the nominated governor for safeguarding.

2. Headteacher/s and the Senior Leadership Team
The Headteacher and Head of Junior School are responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Headteacher has delegated day-to-day responsibility to the Deputy Head. Both the Deputy Head and Head of Junior School are the school's Designated Safeguard Leads.
In particular, the role of the Headteacher/s and the Senior Leadership team is to ensure that:

- staff, in particular the Deputy Head and Assistant Head (Pastoral) are adequately trained about e-safety; and
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

3. E-safety coordinator
The School's Deputy Head and Head of Junior School, are responsible to the Headteacher for the day to day issues relating to e-safety. The Deputy Head and Head of Junior School have responsibility for ensuring this policy is upheld by all members of the school community, and works with IT staff to achieve this. They will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Partnership.

4. IT staff
The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the Deputy Head.

5. Teaching and support staff
All staff are required to sign the Acceptable Use Policy before accessing the school's systems.
As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

6. Pupils
Pupils are responsible for using the school IT systems in accordance with the Acceptable Use Policy, and for letting staff know if they see IT systems being misused.

7. Parents and carers
Giggleswick School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents and carers are responsible for endorsing the school's Acceptable Use Policy.

Education and training

1. Staff: awareness and training
New teaching staff receive information on Giggleswick School's e-Safety and Acceptable Use policies as part of their induction.

All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All supply staff receive information about e-Safety as part of their safeguarding briefing on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's Designated Safeguarding Leads.

2. Pupils: e-Safety in the curriculum
IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas and specifically Computing lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via Curriculum for Life lessons, and PSHCEe and

Computing lessons at the Junior School, by presentations in assemblies, themed events (such as Safer Internet Day) as well as informally when opportunities arise.

At age-appropriate levels, and via Curriculum for Life lessons/PSHHCee and Computing, pupils are taught about their e-safety responsibilities and to look after their own online safety. From Year 7 pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Deputy Head and any member of staff at the school.

At the Junior School, Reception and Key Stage 1 pupils are taught about the importance of passwords, personal information and the potential dangers of 'strangers' online. In Key Stage 2 lessons also cover aspects including privacy settings, posting information online (including images), risks related to online gaming, illegal downloading, viruses/phishing, location sharing, and our digital footprints. The school uses resources produced by CEOP. ChildNet, the NSPCC and Gooseberry Planet.

From Year 7, pupils are also taught about relevant laws applicable to using the internet; such as GDPR and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities and sixth form lectures.

Pupils of all ages are made aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, and GJS Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach their Head of House or the Deputy Head at the Senior School, or form tutor or Head of Junior School, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies. Pupils are also taught to report abuse via the CEOP button. The Duke of York iDEAS badges runs within the senior school where students collect badges on a wide variety of e-safety topics.

3. Parents

The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The weekly newsletter to parents often include hyperlinks to websites that are being used in e-safety lessons as well as relevant articles concerning the latest e-safety issues. The Duke of York Award in digital literacy is also available for parents to complete short courses in.

Policy Statements

1. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff are referred to the BYOD Policy for further guidance on the use of non-school owned electronic devices.

Staff at Giggleswick School are permitted to bring in personal devices for their own use. They may use such devices in the main school staffroom, or a staff office, and only during non-contact time, break-times and lunchtimes.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / carers and under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system.

Pupils – Junior School

To bring a mobile phone or electronic device into school, any pupil must have sought consent from their parents/guardians, and the devices must be named.

Pupils from Reception to Year 6 will have their own devices. These devices are to be used in lessons and other specific learning activities under the supervision of a member of staff. All pupils are referred to the BYOD Policy for further guidance on the use of non-school owned electronic devices.

Pupils need to bring their devices into school each Monday morning and take them home with them each Friday evening.

Pupils may use a mobile phone/tablet during the journey to and from school, the device must not be used to record images that are posted onto social media sites nor should they be used to bully or intimidate other pupils. Once on school premises, the device must be switched off and handed in to the pupil's form teacher. They will then be locked away safely until the end of the day. At the end of the school day, it is the responsibility of the pupil to collect their device from their form teacher. Should they forget to do this, then the device will remain locked safely away. After collection at the end of the day, all devices must not be used on the school site (for example, in the dining hall or in an after-school activity) and if used on the journey home, be used in a responsible manner, abiding to on-line safety rules and the school's code of conduct.

If a pupil needs to contact home, they will be allowed to use a school phone or be supervised using their own phone after it has been collected from the school office. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office if thought necessary.

Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices within Computing and PSHCEe lessons.

For hygiene reasons, pupils must bring a set of headphones to school to be used with their device. These should be named and kept safely in their classroom tubs.

Pupils – Senior School

Students are referred to the BYOD Policy for further guidance on the use of non-school owned electronic devices.

If pupils bring in mobile devices (e.g. for use during the journey to and from school), they should be kept switched off and out of sight all day, and will remain the responsibility of the child in case of loss or damage. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The school has introduced the use of pupil owned tablets as a teaching and learning tool and pupils are required to adhere to the Pupil BYOD Policy when using tablets for schoolwork. In particular, the Pupil BYOD Policy requires pupils to ensure that their use of tablets for school work complies with this policy and the Acceptable Use Policy and prohibits pupils from using tablets for non-school related activities during the school day.

School mobile technologies available for pupil use (including laptops, tablets, cameras, etc.) are stored in a locked cupboard. Access is available via named teachers. Members of staff should sign devices out and in before and after each use by a pupil.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the SENCO and House Master/Mistress to agree how the school can appropriately support such use. The House Master/Mistress will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

2. Use of internet and email

Staff

Staff must not access social networking sites or personal email from school devices or whilst teaching / in front of pupils. Such access may only be made from staff members' own devices whilst in staff-only areas of school.

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.
The school uses a filtering system based on age range, restricting access to websites based on age recommendations and content. The highest level of filtering is enabled for Junior School pupils.

Staff must immediately report to the e-Safety Coordinator the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the e-Safety Coordinator.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Giggleswick School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should school pupils or parents be added as social network 'friends' or contacted through social media.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all schoolwork. Pupils should be aware that email communications through the school network and school email addresses are monitored.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for schoolwork purposes, pupils should contact the IT Team for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to the e-Safety Coordinator.

The school expects pupils to think carefully before they post any information online or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the e-Safety Coordinator. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for schoolwork / research purposes, pupils should contact the IT Team for assistance.

3. Data storage and processing

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

Staff and pupils are expected to save all data relating to their work to their Office365 as per the IT Policy.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by school.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Deputy Head.

4. Password security

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

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every month;
- not write passwords down; and
- not share passwords with other pupils or staff.

5. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the Acceptable Use Policy / IT Policy / Mill House Pre-school Mobile Devices Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
Pupils must not take, use, share, publish or distribute images of others.

Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (see Parent Contract / Acceptable Use Policy for more information).

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6. Misuse

Giggleswick School will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and the Local Safeguarding Partnership. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures (in particular the Safeguarding Policy).

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policies.

The school also has the right to take action against any member of the school community if they are involved in incidents of inappropriate behaviour, that are covered in this policy, when they are out of school and where they involve their membership of the school community (examples would be cyber-bullying, use of images or personal information).

Complaints

As with all issues of safety at Giggleswick School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Deputy Head in the first instance, who will liaise with the leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded and should be reported to the school's e-Safety Co-ordinator and the Designated Safeguarding Lead, Anthony Simpson, in accordance with the school's Child Protection Policy.

Reviewed by:	A Simpson, Deputy Head J Hamilton, Director of Digital Strategy J Mundell, Head of Junior School
Review period:	Annual
Updated:	July 2020
Approved by:	Governors' Pastoral & Boarding Committee, March 2020 - pending
Next review date:	February 2021

Appendix A Giggleswick IT acceptable use policy

Appendix B Giggleswick lending student device policy

Appendix C Giggleswick staff and visitor BYOD policy

Appendix D Giggleswick student BYOD policy

Appendix E Mill House Pre-school Mobile Devices Policy