GIGGLESWICK
SCHOOL

Online Safety Policy

Lead Author(s)	Deputy Head and DSL, Senior School
Reviewed by	Headmaster Head of the Prep School
Approval Committee	Boarding, Wellbeing and Safeguarding, October 2023
Last review	September 2023
Review frequency	Annually
Next review	August 2024
Policy Type	Statutory

Contents

1 INTRODUCTION

Giggleswick School ("the School") believes that online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones, smart watches or games consoles. The internet and information communication technologies are an important part of everyday life and, as a Certified Microsoft Showcase School, are an integral part of our teaching and learning strategies to access and deliver the curriculum, so pupils must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

However, pupils face threats not limited to identity theft, cyberbullying, harassment, grooming, stalking, abuse and radicalisation, whilst the School faces a growing threat from attacks to its IT systems and data breaches – e-crime such as ransomware and phishing is becoming ever more common in the education sector.

The School recognises it has a duty to provide its community with quality internet access to raise education standards, promote achievement, support the professional work of staff and enhance management functions. We recognise our clear duty to ensure that all pupils and staff are protected from potential harm online.

This policy applies to current and emerging technologies used in and outside of school, such as:

- 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.

2 AIMS

The aims of the Online Safety Policy are:

- To promote the welfare and safeguarding of pupils and staff at the School;
- To ensure that pupils are ICT literate and can use the facilities to ensure that their educational provision is supported and enhanced;
- To promote responsible and effective use of electronic communication (including the use of the internet, social media and mobile phone technology);
- To educate pupils and staff about the risks, responsibilities and potential criminal implications involved in the use of technology; and
- To raise awareness and counter instances of cyberbullying.

This policy should be read in conjunction with the following School policies:

- Safeguarding Policy and Procedures
- Acceptable Use Policy (Appendix A to this policy)
- Anti-Bullying Policy (including cyberbullying)
- Behaviour, Rewards and Sanctions Policy; GPS Behaviour Policy

- Data Protection Policy
- Health and Safety Policy
- Mill House Mobile Devices Policy
- PSHE Policy; GPS PSHE Policy
- Pupil BYOD Policy (Appendix D to this policy)
- Relationships and Sex Education Policy
- School Rules
- Staff Code of Conduct
- Staff and Visitor BYOD Policy (Appendix C to this policy)
- Taking, Storing and Using Images of Pupils 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. The School understands its responsibility to educate 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.

The following measures are in place to support this policy:

- The induction of new pupils and staff (including digital training and skills through the Microsoft Education Centre)
- The PSHE programme, including the Year 11 and Sixth Form lecture programmes and PSHE+
- Computing lessons
- Guidance during any academic lesson about use of the internet to embed online safety education
- Specific guidance to pupils, particularly exam classes, about plagiarism
- Parents' Pastoral Briefings
- Guidance to parents and guardians issued in the School's weekly newsletter, *In Touch*
- Robust filtering and regular monitoring of activity across the network and internet
- The Safeguarding Team
- The Pastoral Support Group
- House and Tutor Time

2 SCOPE OF THIS POLICY

This policy applies to all members of the school community, including staff, pupils, parents, residents 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.

This policy and the Acceptable Use Policy (for all staff, visitors and pupils) cover fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.) as well as all BYODs owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

In this policy, the term 'device' refers to a laptop or tablet-type device used to connect to the School's Wi-Fi. The term 'mobile device' refers to a mobile phone or any other device which has cellular connectivity (this can include smart watches such as the Apple Watch).

3 ROLES AND RESPONSIBILITIES

3.1 THE GOVERNING BODY

The Governing Body is responsible for the approval of this policy and for reviewing its effectiveness. The Governing Body (or its nominated sub-committee) will review this policy at least annually, with regular scrutiny from the nominated Governor for Safeguarding.

3.2 HEADMASTER AND THE SENIOR LEADERSHIP TEAM

The Headmaster is responsible for the safety of the members of the school community. The Designated Safeguarding Lead (DSL) is responsible for safeguarding and child protection (including online safety). This is explicit in the role's job description. Both the Deputy Head and Head of the Prep School are the School's DSLs.

In particular, the role of the Headmaster and the Senior Leadership Team is to ensure that:

- Staff, in particular the Deputy Head and Deputy Head (Learning), 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 with the School.

3.3 E-SAFETY COORDINATOR

The School's Deputy Head and Head of the Prep School, are responsible to the Headmaster for day-to-day issues relating to e-safety. The Deputy Head and Head of the Prep School have responsibility for ensuring this policy is upheld by all members of the school community, and work 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 North Yorkshire Safeguarding Children Partnership (NYSCP), CEOP (Child Exploitation and Online Protection), and Childnet International.

3.4 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.

3.5 TEACHING AND SUPPORT STAFF

All staff are required to read 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.

3.6 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.

3.7 PARENTS AND CARERS

The 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.

4 EDUCATION AND TRAINING

4.1 STAFF: AWARENESS AND TRAINING

New teaching staff receive information on the School's Online Safety and Acceptable Use policies as part of their induction.

All teaching staff receive regular information and training on e-safety issues (e.g. online challenges) in the form of INSET training and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

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. When pupils use school computers, staff should make sure pupils are fully aware of the agreement they are making to follow the School's IT policies.

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.

The School has partnered with *Boxphish* to provide regular training on the risks of cyber crime through phishing emails and other associated scams.

4.2 PUPILS: E-SAFETY IN THE CURRICULUM

IT and online resources are used increasingly across the curriculum. The School believes it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. The School continually looks for new opportunities to promote e-safety and regularly monitor and assess pupils' understanding of it.

The School provides opportunities to teach about e-safety within a range of curriculum areas and specifically PSHE and Computing lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE lessons, and PSHE and Computing lessons at the Prep 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 PSHE 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. The Deputy Head talks to Year 7 and 8 pupils each summer term before the holiday period about online risks and the Year 7 induction day has a timetabled online safety lesson as part of the day's programme, delivered by the Deputy Head.

At the Prep 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 approved by the PSHE Association, such as those produced by CEOP, ChildNet, and the NSPCC.

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 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, which describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying). Pupils should approach their Senior House Staff ("SHS") or the Deputy Head at the Senior School, or form tutor or Head of the Prep 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. Specific reference is also made to online hoaxes and challenges, in line with the Government guidance on this matter.

4.3 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.

5 POLICY STATEMENTS

5.1 USE OF SCHOOL AND PERSONAL DEVICES

5.1.1 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 schoolwork. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access. **Passwords must never be shared** as this will allow unauthorised access to the school GS_Corp and GS-Resident networks. These networks are not appropriately filtered for access by pupils. 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 the School are permitted to bring in personal mobile devices for their own use. They may use such devices in the Common Room, 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.

5.1.2 PUPILS – PREP SCHOOL

To bring a mobile device into school, any pupil must have sought consent from their parents/guardians, and such mobile 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 and monitoring 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 may use a mobile device during the journey to and from school; the mobile 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 mobile device must be handed into the school office on arrival each morning and they are kept in a locked cupboard until the end of the day. At the end of the school day, it is the responsibility of the pupil to collect their mobile device from their form teacher. Should they forget to do this, then the mobile device will remain locked safely away. After collection at the end of the day, all mobile 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 School Rules.

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 necessary.

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

Prep School boarders in Catteral House will be permitted to have their phones for a fixed period of time each evening so that they may contact home. This is particularly important for international boarders. Their use is closely monitored by house staff and filtered via the School's BYOD network and filtering system.

5.1.3 PUPILS – SENIOR SCHOOL

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

All pupils in Years 9-11 hand their mobile devices in at morning registration and collect them again at the end of the school day at 6:00pm. This rule applies from Monday to Friday. On Saturdays, pupils in Years 9-11 keep their mobile devices in the morning (in order to communicate any last minute changes to matchday routines/arrangements) but they must 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 mobile devices that communicate over the internet, including smartwatches and other wearable technology. During the week, pupils are permitted to have mobile devices with them on away matches and school trips if deemed appropriate by the trip leader.

In Catteral House, all day pupils in Years 7 and 8 hand their mobile devices in at morning registration and receive them back at 3.45pm at afternoon registration. Arrangements for boarders' mobile devices are handled in house – but no pupil will have access to their mobile device during the teaching day.

No boarding pupil in Years 7-11 has access to their mobile device or device overnight – these are collected in before bedtime and secured in houses.

Sixth form pupils are permitted to keep their mobile devices on their person during the school day. However, mobile devices used openly between these times are liable to confiscation by a

member of staff. Pupils may use mobile devices in houses in designated areas during break times.

The School has introduced the use of pupil-owned devices 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 schoolwork 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 Learning Support Coordinator 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 mobile device at school.

5.2 USE OF INTERNET AND EMAIL

5.2.1 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.

Staff must immediately report to the Deputy Head 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 Deputy Head.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring the 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.

- Staff must only use their school email address when contacting a parent, guardian or carer.
- Staff must only use their school Office 365 account to contact pupils – email or Teams.

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.

5.2.2 PUPILS

All pupils are issued with their own personal password-protected log-in for use with the school email system, as well as providing access to other platforms such as Microsoft Teams. This log-in to school-approved communication platforms such as email and Teams may be regarded as safe and secure and is used for schoolwork. Pupils should be aware that email communications through the school network and school email addresses are monitored.

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 a teacher.

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 an adult. 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 Policy. Pupils should be aware that all internet usage via the School's systems and its Wi-Fi network is filtered and 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. Certain websites are automatically blocked by the School's filtering system. If this causes problems for schoolwork / research purposes, pupils should discuss this with their Tutor who will then contact the IT Team for assistance.

5.3 DATA STORAGE AND PROCESSING

The School takes its compliance with the Data Protection Act 2018 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 account.

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.

5.4 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.

5.5 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).

The School has a separate policy on the Taking, Storing and Using Images of Children and this policy should be referred to for further information.

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 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.

Pupils must not take, use, share, publish or distribute images of others.

5.6 MISUSE

The School will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and North Yorkshire MAST. 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 Policy.

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).

6 CONCERNS AND COMPLAINTS

All members of the School community are reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the School community or which bring the School into disrepute. All members of the community are made aware of the range of online risks that are likely to be encountered including youth produced sexual imagery (YPSI), online/cyber bullying, sexual harassment, access to harmful content, etc. This is highlighted within staff induction and training and educational approaches for pupils.

The Designated Safeguarding Lead (DSL) must be informed of any online safety incidents involving child protection concerns, which will then be recorded. The DSL ensures that online safety concerns are escalated and reported to relevant agencies in line with statutory procedures and guidance within KCSIE 2023 and North Yorkshire Safeguarding Children Partnership (NYSCP) procedures. The School informs parents/guardians of any incidents or concerns as and when required.

Any complaint about staff misuse is referred to the Headmaster and allegations against a member of staff's online conduct may lead to disciplinary action, and may be discussed with the LADO (Local Authority Designated Officer) team. Where there is cause for concern or fear that illegal activity has taken place or is taking place then the School will contact North Yorkshire Police via 101, or 999 if there is immediate danger or risk of harm. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to North Yorkshire Police.

Parents and pupils will need to, and are expected to, work in partnership with the School to resolve any issues that arise.

Any complaints by parents or pupils should follow the School's Complaints Procedures which set out the process for raising a complaint. The procedures are available on the School's Policies website page.

APPENDIX A ACCEPTABLE USE POLICY

This acceptable use policy applies to all members of the school community, including staff, pupils, parents, and visitors ("Users"). In this policy, 'staff' includes teaching and non-teaching staff, governors, and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the School, including occasional volunteers.

A.1 ONLINE BEHAVIOUR

All members of the School community should follow these principles in all online activities:

- Ensure that online communication, and any content shared online, is respectful of others and composed in a way one would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as one's own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts, to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

A.2 USE OF THE SCHOOL'S IT SYSTEMS

Whenever users access the School's IT systems (including by connecting one's own device to the network), the following principles apply:

- Only access school IT systems using one's own username and password. Do not share the username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that they do not have permission to access.
- Do not attempt to install software on, or otherwise alter, School IT systems.
- Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the School monitors use of the School's IT systems, and that the School can view content accessed or sent via its systems.

A.3 PASSWORDS

Passwords protect the School's network and computer system and are an individual's responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as widely-used personal passwords. Users should not let anyone else know their password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. Users should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which they do not have access rights.

A.4 USE OF PROPERTY

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. Users must report any faults or breakages without delay to the IT department using the *ITHelpdesk* email facility.

A.5. USE OF SCHOOL SYSTEMS

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Users must be aware of the school's right to monitor and access web history and email use.

A.6 USE OF PERSONAL DEVICES OR ACCOUNTS AND WORKING REMOTELY

All official school business must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the IT department.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies, including password protection and encryption.

A.7 MONITORING AND ACCESS

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the School where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, whether or not such use is permitted, may be confiscated and examined under such circumstances. The School may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy.

A.8 COMPLIANCE WITH RELATED SCHOOL POLICIES

Users must comply with the following policies:
School's Online Safety Policy, Safeguarding Policy and Procedures, Data Protection Policy, Data Retention Policy, BYOD Policy, Taking, Storing and Using Images of Children Policy and Data Breach Reporting Policy.

A.9 RETENTION OF DIGITAL DATA

Staff and pupils must be aware that all emails sent or received on school systems will be kept in archive, whether or not deleted, and email accounts will be closed, and the contents archived within 30 days of that person leaving the school. An auto-response may be set on their account for the first 30 days.

Important information that is necessary to be kept should be held on the relevant personnel or pupil file, and not kept in personal folders, OneDrive, archives or inboxes. It is therefore the responsibility of the staff involved in the handover process to ensure that important information (or indeed any personal information that the departing member of staff wish to keep, in line with school policy on personal use) is retained in the correct place or, where

applicable, provided to the relevant colleague. That way, no important information should ever be lost as a result of the school's email deletion protocol.

Line managers are responsible for removing access to all third-party software and websites for any member of staff who leaves the School. This should be completed by midnight on the staff member's final day of service.

If line managers have appropriate reasons for the protocol not to apply, or need assistance in how to retain and appropriately archive data, they should contact the IT Department.

A.10 BREACH REPORTING

The law requires the School to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the School regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the School's systems, e.g. through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The School must generally report personal data breaches to the ICO without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, they should in the first instance contact the Bursar or a teacher, respectively.

Data breaches will happen to all organisations, but the School must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The School's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be treated as a disciplinary offence.

A.11 BREACHES OF THIS POLICY

A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures. In addition, a deliberate breach may result in the school restricting a user's access to School IT systems.

If users become aware of a breach of this policy or the Online Safety Policy, or they are concerned that a member of the School community is being harassed or harmed online, they should report it to the Bursar or the Deputy Head. Reports will be treated in confidence.

A.12 ACCEPTANCE OF THIS POLICY

Users will automatically be accepting the School's acceptable use policy when they sign-in to the School network or use their device for school business.

APPENDIX B LENDING PUPIL DEVICE POLICY

Agreement for Short-term Loan of a device to Giggleswick School pupils

Date:

Between:

(1) Giggleswick School (‘**the School’**); and

(2) [insert the name(s) [and email addresses] of the pupil's parents or guardians] (‘**you’**).

Your pupil: [insert name of pupil]

Device: [Describe the device]

Background

The School has a policy of making devices available for short-term loan to pupils to use in the classroom, for homework, and for independent study. Loan is only usually available in a short-term basis to cover, for example, a lost or damaged device. To make sure that pupils have access to these devices when they need them, pupils can borrow a device on a short-term basis during his or her time as a pupil of the School, subject to subject to the pupil's parent(s) or guardian(s) agreeing to certain conditions. This is an agreement between you and the School and sets out the terms on which the School will permit your child to use the Device. Please indicate your acceptance of the terms by signing where indicated below.

Agreed terms

1 Commencement and termination

1.1 By signing this agreement where indicated below, you offer to be bound by its terms. The School's acceptance of your offer occurs when the School provides the Device to you or your pupil, at which point this agreement commences and becomes binding on you and the School.

1.2 This agreement will terminate, unless terminated earlier, when you or your child return the Device to the School in accordance with clause 6. Rights and liabilities accrued before termination, including (without limitation) your liability to pay any money you owe the School under clause 5.5 or 6.3, will be unaffected by termination of this agreement.

2 Loan of the Device

2.1 In consideration for you complying with your obligations under this agreement, the School will lend the Device to you for use by your pupil for the purposes described in clause 3.1below. The loan of the Device will begin when the School provides your or your child with the Device, and will end on the date you are required to return the Device to the School in accordance with clause 6.

2.2 The Device will remain the property of the School at all times.

3 Use of the Device

3.1 The School will ensure that the Device is fit for use by your child for the purposes described in clause 3.3 below whilst it is on loan to you.

3.2 The School will ensure that the Device is capable of using the School's internet connection on the School's premises whilst it is on loan to you, but will not be responsible for ensuring that the Device is capable of connecting to the internet elsewhere, or that the Device is compatible with your computer systems.

3.3 Your child may take the Device out of school whilst it is on loan to you, provided that you ensure your pupil brings the Device with him or her every day he or she attends school.

3.4 You will ensure that the Device is only used by your child, and only for the following purposes:

3.4.1 for use in class as directed by the teacher leading the class;

3.4.2 for use in preparing and submitting homework;

3.4.3 for independent study;

3.4.4 for accessing applications and networks made available to your pupil by the School; and

3.4.5 for your pupil's personal, non-commercial use subject to clauses 3.5 to 3.8 below.

3.5 You will ensure that your child's use of the Device complies with the School's policies on e-safety, acceptable use of computer systems, bullying and harassment as notified to you by the School from time-to-time (**the Policies**).

3.6 You will ensure that your pupil follows any instructions issued by the School regarding use of the Device.

3.7 You will not, and will ensure that your pupil does not, use the Device for any form of financial transaction or dealing, including (without limitation) online shopping or banking.

3.8 You will not, and will ensure that no one else, downloads or installs software or media files to the Device from external sources without authorisation from the School. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files.

4 Monitoring

4.1 You agree that the School may monitor use of the Device in the same way that the School monitors use of its other computer systems in accordance with the Policies, including (without limitation) viewing any data stored on or accessed via the Device.

4.2 The School may remotely make changes to the Device and any software installed on the Device at any time, including (without limitation) making the Device inoperable.

4.3 You agree that any data stored on the Device shall be the property of the School, and that the School may copy, store, modify, delete, or otherwise use that data in any way it reasonably considers appropriate.

5 Repair and safekeeping of the Device

5.1 You will keep, and will ensure that your child keeps, the Device safe at all times during the term of this agreement, including (without limitation) whilst the Device is being used on School premises.

5.2 If the Device is stolen during the term of this agreement, you will report the theft to the police and the School as soon as reasonably practical after you become aware of the theft. You will promptly provide the School with any information that the School reasonably requires in relation to the theft, including (without limitation) any crime reference number provided to you by the police.

5.3 During the term of this agreement if the Device is lost or any material defect occurs in it:

5.3.1 you will notify the School in writing as soon as reasonably practical; and

5.3.2 in the case of a defect, you will ensure that the Device is returned promptly to the School;

5.4 Provided you comply with clauses 5.2 and 5.3, the School will, at its discretion, lend you a replacement device in the case of loss or theft or in the case of a defect either (at its option) repair the Device or lend you a replacement.

5.5 If a material defect occurs in the Device during the term of this agreement as a result of anything done to the Device by you or your pupil or a third party (other than an employee or contractor of the School), or if the Device is lost or stolen as a result of your negligence or the negligence of your pupil, you will pay the School's reasonable costs of repairing or replacing the Device (as the case may be). In any other case, the School will bear the costs of repair or replacement.

5.6 References in this agreement to the Device are to be read as references to any replacement provided by the School.

6 Returning the Device

6.1 The School may give you written notice to return the Device to the School. Such a notice will specify a date for the return of the Device.

6.2 Upon the earlier of i) the last day on which your pupil is a pupil of the school, ii) the date specified in the notice referred to at clause 6.1, or iii) the termination of this agreement (for any reason), you will return, or ensure that your pupil returns, the Device to the School.

6.3 If you do not return, or ensure that your pupil returns, the Device to the School, in accordance with this clause 6 you will pay the School's reasonable costs of procuring a replacement.

7 The School's liability

7.1 The School will not be liable to you (whether in contract, tort, or in any other way) for any loss, injury or damage that arises out of or in connection with any defect in the Device. However, this does not exclude the School's liability for death or personal injury caused by negligence on the part of the School or for fraud on the part of the School.

8 Other terms

8.1 You will send any notices under this agreement to the Bursar at bursar@giggleswick.org.uk.

8.2 This agreement and the documents referred to in it contain the entire agreement between you and the School in relation to the Device, and replace any earlier agreement about the Device.

8.3 Your liability under this agreement is joint and several if there are more than one of you.

8.4 This agreement and any dispute arising out of or in connection with it (including non-contractual disputes and claims) will be governed and construed according to the law of England and Wales, and will be subject to the non-exclusive jurisdiction of the Courts of England and Wales.

By signing this agreement you offer to be legally bound by the terms set out above.

Signed by: [NAME OF PARENT/GUARDIAN] ……

Date: ……

Signed by: [NAME OF PARENT/GUARDIAN] ……

Date: ……

(EACH PARENT/GUARDIAN NAMED AT THE FRONT OF THIS AGREEMENT SHOULD SIGN HERE.)

APPENDIX C STAFF AND VISITOR BYOD POLICY

This policy is intended to address the use by staff members (including volunteers and Governors) and visitors to the School of non-school owned devices to access the internet via the School's internet connection, to access or store school information, or to make photographs, video, or audio recordings at school. These devices include smart phones, tablets, laptops, wearable technology and any similar devices. These devices are referred to as 'mobile devices' in this policy.

Sections one to three and five of this policy apply to all school staff and to visitors to the School. The rest of the policy is only relevant to school staff.

This policy is supported by the Acceptable Use Policy.

The School's Governing Body is responsible for the approval of this policy and for reviewing its effectiveness. They, or its nominated sub-committee, will review this policy at least annually.

C.1 USE OF MOBILE DEVICES AT SCHOOL

Staff and visitors to the School may use their own mobile devices in a discrete fashion and usually when they are not in the presence of pupils or visible by pupils. Devices can only be used in the classroom with the permission of the Teacher.

Staff and visitors to the School are responsible for their mobile device at all times. The School is not responsible for the loss or theft of or damage to the mobile device or storage media on the device (e.g. removable memory card) howsoever caused. Reception must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged.

Mobile devices must be turned off when in a prohibited area and/or at a prohibited time and must not be taken into controlled assessments and/or examinations, unless special circumstances apply.

The School reserves the right to refuse staff and visitors' permission to use their own mobile devices on school premises. Personal devices are not permitted for use in the Prep School or Mill House Pre-school in classrooms or areas accessed by pupils.

C.2 USE OF CAMERAS AND AUDIO RECORDING EQUIPMENT

The Policy on Taking, Storing and Using Images of Children should be referred to.

Parents and carers may take photographs, videos or audio recordings of their children at school events for their own personal use.

Other visitors and staff may use their own mobile devices to take photographs, video, or audio recordings in school provided they first obtain permission to take photographs, films or recordings of the relevant individuals. This includes people who might be identifiable in the background.

To respect everyone's privacy and in some cases protection, photographs, video, or audio recordings should not be published on blogs, social networking sites (i.e. via tagging) or in any other way without the permission of the people identifiable in them. Parents or carers should avoid commenting on activities involving pupils other than their own in photographs, video, or audio, and other visitors and staff should comment.

No one must use mobile devices to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third-party acting remotely to take photographs, video, or audio recordings in school. Staff must comply with the School's Code of Conduct and Anti-Bullying policies when making photographs, videos, or audio recordings and they must not store images or recordings of pupils on their personal devices.

C.3 ACCESS TO THE SCHOOL'S INTERNET CONNECTION

The School provides a wireless network that staff and visitors to the School may use to connect their mobile devices to the internet. Access to the wireless network is at the discretion of the School, and the School may withdraw access from anyone it considers is using the network inappropriately.

The School cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. In particular, staff and visitors are advised not to use the wireless network for online banking or shopping.

The School is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the School's wireless network. This activity is taken at the owner's own risk and is discouraged by the School. The School will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the School's wireless network.

C.4 ACCESS TO SCHOOL IT SERVICES

School staff are permitted to connect to or access the following school IT services from their personal mobile devices:

- Office 365
- iSAMS
- SOCS
- School Portal
- CPOMS (selected staff only)

Staff may use the systems listed above to view school information via their mobile devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their mobile devices. In some cases, it may be necessary for staff to download school information to their mobile devices in order to view it (for example, to view an email attachment). Staff must delete this information from their devices as soon as they have finished viewing it.

Staff must only use the IT services listed above and any information accessed through them for work purposes. School information accessed through these services is confidential, in particular, information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to or distribution of confidential information should be reported to the School's IT team or HR department as soon as possible.

Staff must not send school information to their personal email accounts or similar messaging type services, e.g. WhatsApp, and storage accounts.

If in any doubt, a device user should seek clarification and permission from the School's IT Department before attempting to gain access to a system for the first time. Users must follow the written procedures for connecting to the school systems.

C.5 MONITORING THE USE OF MOBILE DEVICES

The School may use technology that detects and monitors the use of mobile and other electronic or communication devices which are connected to or logged on to our wireless network or IT systems. By using a mobile device on the School's IT network, staff and visitors to the School agree to such detection and monitoring. The School's use of such technology is for the purpose of ensuring the security of its IT systems and the safeguarding of its pupils.

The information that the School may monitor includes (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms (including passwords), information uploaded to or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Staff who receive any inappropriate content through school IT services or the School internet connection should report this to the IT Department as soon as possible.

C.6 SECURITY OF STAFF MOBILE DEVICES

Staff must take all sensible measures to prevent unauthorised access to their mobile devices, including but not limited to the use of a PIN, pattern or password to be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time.

Staff must never attempt to bypass any security controls of the school systems or others' own devices.

Staff are reminded to familiarise themselves with the School's Online Safety Policy, the Staff Code of Conduct, and acceptable use of IT policies which set out in further detail the measures needed to ensure responsible behaviour online.

Staff must ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up-to-date.

C.7 COMPLIANCE WITH DATA PROTECTION POLICY

Staff compliance with this BYOD policy is an important part of the School's compliance with the Data Protection Act 2018. Staff must apply this BYOD policy consistently with the School's Data Protection Policy.

C.8 SUPPORT

The School takes no responsibility for supporting staff's own devices; nor has the School a responsibility for conducting annual PAT testing of personally owned devices.

C.9 COMPLIANCE, SANCTIONS AND DISCIPLINARY MATTERS FOR STAFF

Non-compliance of this policy exposes both staff and the School to risks. If a breach of this policy occurs, the School will respond immediately by issuing a verbal then written warning to the staff member. Guidance will also be offered. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the mobile device in question may be confiscated and/or permission to use the device on School premises will be temporarily withdrawn. For persistent breach of this policy, the School will permanently withdraw permission to use user-owned devices in school. Safeguarding concerns about adults working in School will be dealt with in line with the published Safeguarding Policy and Procedures.

C.10 INCIDENTS AND RESPONSE

The School takes any security incident involving a staff member's or visitor's personal device seriously and will always investigate a reported incident. Loss or theft of the mobile device

should be reported to Reception in the first instance. Data protection incidents should be reported immediately to the Bursar at bursar@giggleswick.org.uk.

APPENDIX D PUPIL BYOD POLICY

D.1 INTRODUCTION

This policy is intended to address pupil's use of non-school owned electronic devices to access the internet via the School's internet connection, to access or store school information, or to make photographs, video, or audio recordings at school. These devices include smart phones, tablets, laptops, wearable technology and any similar devices. Additionally, any device with cellular connectivity is defined as a mobile phone even if the SIM card has been removed. Pupils unsure whether their device is captured by this policy should check with the Deputy Head. These devices are referred to as 'mobile devices' in this policy.

This policy is supported by the Acceptable Use Policy.

The Governing Body of the School, or its nominated sub-committees, will review this policy at least annually.

For many young people today the ownership of a mobile phone/digital device is considered a necessary and vital part of their social life. When used creatively and responsibly the smart phone/digital device has great potential to support a pupil's learning experiences.

D.2 USE OF MOBILE DEVICES AT THE SCHOOL

Pupils are allowed to bring mobile devices into school. If they choose to do so, it is on the understanding that they agree with the following limitations on its use, namely:

Pupils may use their own mobile device in the following locations:

- In the classroom with the permission of the teacher.
- In the School environs at permissible times (see below) - common rooms, boarding houses, etc.

Pupils may not bring any mobile devices in the following locations:

- Changing facilities.
- Examination rooms.

The mobile device must be kept out of sight in public areas, e.g. the Flat, the dining hall and the Sharpe Library, unless it is being used as a learning resource.

When use of a mobile device in lessons has been sanctioned, pupils must use it positively and for the agreed task. Disrupting the learning of others through use of the mobile device will not be tolerated.

Mobile device use in houses will be at the discretion of the Housemaster or Housemistress.

If asked to do so, content on the mobile device (e.g. messages, emails, pictures, videos, sound files) will be shown to the designated members of staff.

Mobile devices should be handed in to the duty staff overnight in Years 7-11, as per the School Rules.

Pupils are responsible for their mobile device at all times. The School is not responsible for the loss or theft of or damage to the mobile device or storage media on the device (e.g. removable memory card) howsoever caused. Reception must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged.

At the Prep School, all devices for learning will remain in the pupil's classroom at all times, but may be taken home on weekends. Pupils who require a mobile phone should hand these into form staff or to the school secretary each morning, and will have these returned at the end of the school day. They may only be used on buses and out of school. Devices for learning are only to be used under the direction and supervision of a member of staff.

Mobile devices must be turned off when in a prohibited area and/or at a prohibited time and must not be taken into controlled assessments and/or examinations, unless special circumstances apply.

The School reserves the right to refuse pupils permission to use their own mobile devices on school premises.

D.3 ACCESS TO THE SCHOOL'S INTERNET CONNECTION

The School provides a wireless network that students may use to connect their mobile devices to the internet. Access to the wireless network is at the discretion of the School, and the School may withdraw access from anyone it considers is using the network inappropriately.

The School cannot guarantee that the wireless network is secure, and pupils use it at their own risk. In particular, pupils are advised not to use the wireless network for online banking or shopping.

The School is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the School's wireless network. This activity is taken at the owner's own risk and is discouraged by the School. The School will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the School's wireless network.

D.4 MONITORING THE USE OF MOBILE DEVICES

The School may use technology that detects and monitors the use of mobile and other electronic or communication devices which are connected to or logged on to our wireless network or IT systems. By using a mobile device on the School's IT network, pupils agree to such detection and monitoring. The School's use of such technology is for the purpose of ensuring the security of its IT systems, and the safeguarding of its pupils.

The information that the School may monitor includes (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms (including passwords), information uploaded to or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Pupils who receive any inappropriate content through school IT services or the school internet connection should report this to a member of teaching staff as soon as possible who will then contact the IT Department if appropriate.

D.5 MISUSE OF MOBILE DEVICES

The following are examples of misuse but are not exhaustive. 'Misuse' will be at the discretion of the Headmaster or Head of the Prep School:

- The deliberate engineering of situations where people's reactions are filmed or photographed in order to humiliate, embarrass and intimidate by publishing to a wider audience via social media.
- Bullying by text, image and email messaging.

- The use of a mobile device for 'sexting' or transmitting Youth Produced Sexual Imagery (the deliberate taking and sending of provocative images or text messages).
- Pupils posting material on social network sites with no thought to the risks to their personal reputation and sometimes with the deliberate intention of causing harm to others.
- Making disrespectful comments, misrepresenting events or making defamatory remarks about staff or other pupils.
- General disruption to learning caused by pupils accessing mobile device in lessons.
- The use of mobile devices in public areas which is affecting the social interactions of the pupils and staff at the School.
- Pupils phoning parents immediately following an incident so that the ability of staff to deal with an incident is compromised.
- Publishing photographs of vulnerable pupils, who may be on a child protection plan, where this may put them at additional risk.

D.6 DEALING WITH BREACHES

Misuse of the mobile phone/digital device will be dealt with using the same principles set out in the School's behaviour policy and the School Rules, with the response being proportionate to the severity of the misuse.

Pupils are aware that misuse may lead to the confiscation of their mobile phone/digital device, communication with parents and the imposition of other sanctions up to and including exclusion from the School. If the offence is serious, it will be reported to the Police.

Where it is deemed necessary to examine the contents of a mobile phone/digital device this will be done by a designated member of staff (Headmaster/Deputy Head/Head of the Prep School), and should follow the protocol of searching any pupil's possessions.

The action will be properly recorded in case it later becomes evidence of criminal activity. The record will include the time, who was present and what is found.

D.7 UNACCEPTABLE USE

The School will consider any of the following to be unacceptable use of the mobile device and a serious breach of the School's behaviour policy, resulting in sanctions being taken.

- Photographing or filming other pupils or members of staff without their knowledge or permission.
- Photographing or filming in toilets, changing rooms and similar areas.
- Bullying, harassing or intimidating staff or pupils by the use of text, email or multimedia messaging, sending inappropriate messages or posts.
- Refusing to switch a mobile device off or handing over the mobile device at the request of a member of staff.
- Using the mobile device outside school hours to intimidate or upset pupils and staff will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.
- Using a mobile device outside school hours in such a way that it undermines the stability of the School and compromises its ability to fulfil the stated aim of providing 'a clear moral and ethical lead'.

D.8 SANCTIONS

Pupils and parents are notified that appropriate action will be taken against those who are in breach of the acceptable use guidelines, following the School's behaviour policy. In addition, pupils and their parents should be clear that the School is within its rights to confiscate the mobile device where the guidelines have been breached.

Using the mobile phone/digital device outside school hours to intimidate or upset pupils and staff or undermine the stability of the School in any way will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.

- If a phone/digital device is confiscated, School will make it clear for how long this will be and the procedure to be followed for its return.
- Pupils should be aware that the police will be informed if there is a serious misuse of the mobile phone/digital device where criminal activity is suspected.
- If a pupil commits an act which causes serious harassment, alarm or distress to another pupil or member of staff the ultimate sanction may be permanent exclusion. School will consider the impact on the victim of the act in deciding the sanction.

D.9 DEVICE CONFISCATION

Staff may confiscate mobile devices if they have been used inappropriately. The length of confiscation is at the discretion of the pupil's SHS and may range from as little as one day to one week. Day pupil's device will always be returned to them at the end of the day but it may be that the pupil then must surrender the device on arrival the next morning until the end of that day. Boarders' devices will be held by SHS for the duration of the confiscation period. Boarders will always be permitted to make calls home, either using their phone for a specified period of time or via the house phone.

The School will ensure that confiscated equipment is stored in such a way that it is returned to the correct person

Where a pupil persistently breaches expectations, following a clear warning, the Headmaster/Head of the Prep School may impose an outright ban from bringing a mobile device to school. This may be a fixed period or permanent ban.

D.10 WHERE THE MOBILE DEVICE HAS BEEN USED FOR AN UNACCEPTABLE PURPOSE

The Headmaster or a designated staff member (Deputy Head/Head of the Prep School) will have the right to view files stored in confiscated equipment and if necessary, seek the cooperation of parents in deleting any files which are in clear breach of these guidelines unless they are being preserved as evidence.

If required, evidence of the offence or suspected offence will be preserved, preferably by confiscation of the device and keeping it secure or by taking photographs of the screen.

School will consider whether an incident should be reported to social services.

The designated staff member should monitor repeat offences to see if there is any pattern in the perpetrator or the victim which needs further investigation.

D.11 SECURITY OF PUPIL MOBILE DEVICES

Pupils must take all sensible measures to prevent unauthorised access to their mobile devices, including, but not limited to, the use of a PIN, pattern or password to be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time. Pupils must never attempt to bypass any security controls in school systems or others' own devices.

Pupils are reminded to familiarise themselves with the school's Online Safety Policy, and Acceptable Use of IT Policy which set out in further detail the measures needed to ensure responsible behaviour online.

Pupils should ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up-to-date.

D.12 COMPLIANCE WITH DATA PROTECTION POLICY

Compliance with this BYOD policy is an important part of the School's compliance with the Data Protection Act 2018. Staff must apply this BYOD policy consistently with the School's Data Protection Policy.

D.13 SUPPORT

The School takes no responsibility for supporting pupils' own devices; nor has the School a responsibility for conducting annual PAT testing of personally-owned devices.

D.14 INCIDENTS AND RESPONSE

The School takes any security incident involving a pupil's personal device seriously and will always investigate a reported incident. Loss or theft of the mobile device should be reported to Reception in the first instance. Data protection incidents should be reported immediately to the Bursar.