




THE BISHOP'S STORTFORD HIGH SCHOOL

ONLINE SAFETY POLICY

| | | | |
|-----------------------------|-------------|-----------------------|--|
| Date of last review: | Summer 2021 | Review period: | 2 years |
| Date of next review: | July 2023 | Owner: | Student Welfare & Development |
| | | Approval: |  |



TBSHS: A truly all-round education



Contents

| | |
|---|----|
| 1. Introduction..... | 1 |
| 2. Responsibilities..... | 1 |
| 3. Scope of policy..... | 1 |
| 4. Policy and procedure..... | 2 |
| Use of email..... | 2 |
| Visiting online sites and downloading..... | 2 |
| Storage of Images/Recordings..... | 3 |
| Use of personal mobile devices (including phones)..... | 3 |
| New technological devices..... | 4 |
| Reporting incidents, abuse and inappropriate material..... | 4 |
| 5. Curriculum..... | 4 |
| 6. Staff and Governor Training..... | 5 |
| 7. Working in Partnership with Parents/Carers..... | 5 |
| 8. Records, monitoring and review..... | 6 |
| 9. Appendices of the Online Safety Policy..... | 6 |
| Appendix A - Agreement - Internet/IT Equipment/Online Safety/Mobile Devices - Acceptable Use (Staff, governors, trainee teachers, peripatetic teachers, coaches, supply teachers, etc)..... | 7 |
| Appendix B - Requirements for Visitors, Volunteers and Parent/Carer helpers..... | 11 |
| Appendix C - Students Years 07 to 11 - Internet/IT Equipment/Mobile Devices - Acceptable Use Agreement (Student and Parent/Carer)..... | 12 |
| Appendix D - Students Years 12 to 13 - Internet/IT Equipment/Mobile Devices - Acceptable Use Agreement (Student and Parent/Carer)..... | 15 |
| Appendix E - Online safety policy guide - Summary of key parent/carer responsibilities..... | 18 |
| Appendix F - Guidance on the process for responding to cyberbullying incidents..... | 19 |
| Appendix G - Guidance for staff on preventing and responding to negative comments on social media..... | 20 |
| Appendix H - Online safety incident reporting form..... | 21 |
| Appendix I - Online safety incident record..... | 23 |
| Appendix J - Online safety incident log..... | 25 |



TBSHS: A truly all-round education



1. Introduction

TBSHS recognises that internet, mobile and digital technologies provide a good opportunity for children and young people to learn, socialise and play, provided they are safe. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** students, staff and governors will be able to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some students may require additional support or teaching; including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in the safeguarding of children.

2. Responsibilities

The Headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The online safety co-ordinator in this school is the Assistant Headteacher with pastoral responsibility for Key Stage 4. All breaches of this policy must be reported to the online safety co-ordinator.

All breaches of this policy that may have put a child at risk must also be reported to a Designated Safeguarding Person. Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network and equipment then they must adhere to the school's online safety procedures and acceptable use agreements. If the organisation is operating in school time or when students are on site in the care of the school, then the safeguarding of students is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

3. Scope of policy

The policy applies to:

- students
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that students who receive part of their education off site or who are on a school trip or residential are safe online. The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their children to behave appropriately and keep themselves safe online. This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, GDPR, health and safety, home-school agreement, behaviour, anti-bullying and PSHCE/RSE policies.

4. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk. The school expects everyone to use the internet, and mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations of appropriate online behaviour and use of technology outside of school for students, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and governors should use a school email account or Governor Hub for all official communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact students, parents or conduct any school business using a personal email address. Students may only use school approved accounts on the school system and only for educational purposes. Where required parent/carer permission will be obtained for the account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parental permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000 and/or GDPR subject access requests.

Staff, governors and students should not open emails or attachments from suspect sources and should report their receipt to Network Support.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

- Staff must review the suitability, security and appropriateness of websites, software and apps before their use in school or before recommending them to students. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.
- Staff must only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with students/ families.
- When working with students searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
 - Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
 - Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
 - Adult material that breaches the Obscene Publications Act in the UK
 - Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, disability, sexual orientation, age and marital status
 - Promoting hatred against any individual or group from the protected characteristics above
 - Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
 - Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect
- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the school network and internet connection, including

- the creation, propagation and/or transmission of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

Only a school device may be used to conduct school business outside of school. The only exception would be where a closed, monitorable system has been set up by the school for use on a school authorised personal device.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the Network Manager or online safety coordinator.

Storage of Images/Recordings

Photographs and videos provide valuable evidence of students' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. For students aged 13 and above, consent for images is decided upon and signed by the student. (See GDPR policy for greater clarification).

Photographs and images of students are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by the Pastoral Deputy Headteacher. Staff and students may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own children.

Staff and other professionals working with students, must only use school approved equipment to record images of students whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of students. Under no circumstance does the school allow a member of staff to contact a student or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from online safety co-ordinator. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. In lesson times all such devices must be switched off. Under no circumstance should students use their personal mobile devices/phones to take images of

- any other student unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage or theft on school premises of any personal mobile device.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Personal mobiles must never be used to access school emails and data. The only exception would be where a closed, monitorable system has been set up by the school for use on a school authorised personal device.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, students and staff should not assume that new technological devices will be allowed in school and should check with the Network Manager before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a student or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the student or adult must report the incident immediately to the first available member of staff, the DSP, Headteacher or online safety co-ordinator. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSP will refer details to social care or the police.

5. Curriculum

Online safety is embedded within our curriculum. The school provides a comprehensive curriculum for online safety which enables students to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for students to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Students are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)
- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, IM/email address) and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images
- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

6. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with students.

Any organisation working with children based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix A).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix A).

Guidance is provided for occasional visitors, volunteers and parent/carer helpers (Appendix B).

7. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website and by other means.

Parents/carers are asked to read, discuss and co-sign with each child the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided and is available in Appendix E. The Acceptable Use Agreement explains the school's expectations and student and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to students and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. Online safety incident recording formats are provided in appendices H, I and J.


The school supports students and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition governors ensure they have sufficient, quality information to enable them to make a judgement about the "fitness for purpose" of this policy on an annual basis.

9. Appendices of the Online Safety Policy

- A. Agreement - Internet/IT Equipment/Online Safety/Mobile Devices - Acceptable Use (Staff, governors, trainee teachers, peripatetic teachers, coaches, supply teachers, etc)
- B. Requirements for Visitors, Volunteers and Parent/Carer helpers
- C. Students Years 07 to 11 - Internet/IT Equipment/Mobile Devices - Acceptable Use Agreement (Student and Parent/Carer)
- D. Students Years 12 to 13 - Internet/IT Equipment/Mobile Devices - Acceptable Use Agreement (Student and Parent/Carer)
- E. Online safety policy guide - Summary of key parent/carers responsibilities
- F. Guidance on the process for responding to cyberbullying incidents
- G. Guidance for staff on preventing and responding to negative comments on social media
- H. Online safety incident reporting form
- I. Online safety incident record
- J. Online safety incident log

Appendix A - Agreement - Internet/IT Equipment/Online Safety/Mobile Devices - Acceptable Use (Staff, governors, trainee teachers, peripatetic teachers, coaches, supply teachers, etc)

| | | | | |
|--|--|--|----------|-----------|
|  | THE BISHOP'S STORTFORD HIGH SCHOOL London Road, Bishop's Stortford, Hertfordshire, CM23 3LU, UK. +44 1279 868686 | Agreement Internet/IT Equipment/Online Safety/Mobile Devices - Acceptable Use (Staff, governors, trainee teachers, peripatetic teachers, coaches, supply teachers, etc) | E | V20191112 |
|--|--|--|----------|-----------|

Agreement - Internet/IT Equipment/Online Safety/Mobile Devices - Acceptable Use (Staff, governors, trainee teachers, peripatetic teachers, coaches, supply teachers, etc)

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff, governors, trainees, peripatetics, coaches and supply are aware of their responsibilities in relation to their use. All staff, governors, trainees, peripatetics, coaches and supply are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the DSP and/or Network Support. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

All users need to understand that everything that they search for, access, post or receive online can be traced now and in the future. Their activity can be monitored and logged and if necessary shared with staff, parents/carers and/or the police.

The School's E-Safety, Internet Use and Data Security Policies have been drawn up to protect all parties - Students, Staff and the school. All students and staff using the IT equipment and Internet at the school must sign the Acceptable Use Agreement before access will be given. The network is owned by the school and access is given on the understanding that it is for educational use only.

This agreement forms part of your professional and safeguarding responsibility in the school. You must read this agreement in conjunction with the school's online safety policy and GDPR policy. Once you have read these, you must sign and submit this agreement. This will be kept on record in the school. You should retain your own copy for reference. It is highly recommended that you also read "General Data Protection Regulation (GDPR) - TBSHS Do's and Don'ts".

Main Principles:

- All users of the internet are responsible for their behaviour and any communications sent over it;
- All users need to realise it is essential that they maintain a good online reputation and digital footprint;
- No activity shall be undertaken which could either threaten the integrity of the school ICT systems or attack or corrupt other systems;
- Only use school IT equipment for school purposes;
- Treat all equipment with respect;
- Access must only be made through authorised accounts;
- Users may not make purchases or enter into contracts over the Internet using school systems;
- Online chat is not permitted, either across the school network or over the internet;
- Students contacting teachers electronically, other than via the school e-mail system on a school related matter, is strictly forbidden;
- Posting anonymous messages and forwarding chain letters is not permitted;
- Use of the Internet to access inappropriate material such as pornographic, racist or offensive material is not permitted;
- Copyright of material must be respected.

Copyright/Ownership

I will respect the privacy and ownership of others' work online and will adhere to copyright at all times.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the Online Safety Lead and/or DSP and an incident report completed.

Online Conduct

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

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see Online Safety Policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Network Support.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, could be made available to my line manager, Headteacher and/or others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to students and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the School.

Social Networking

Information can be shared with students (over 13 for social media) and parents/carers through the school's official website, school email and/or social network site/page e.g. Twitter, but never through a personal account or site.

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become "friends" with students and/or parents/carers on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with students and/or parents/carers. Please be aware that former students aged 18 (and over) can still be classified as "vulnerable" young people up to the age of 25.

In my professional role in the school, I will never engage in 1-1 exchanges with students or parent/carers on personal social network sites.

When using social networking for personal use I will ensure my settings are not public.

My private account postings will never undermine or disparage the school, its staff, governors, students and/or parents/carers. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords And Security

I am aware that my level of access to the internet and/or school systems is determined by the school. I must not attempt to access any area that has been protected from me by way of restricted permissions or hidden directories, folders or files on any computer system owned by the school.

If I have access of any kind, I understand that there is no occasion when a password should be shared with anyone else (unless it is a purposely set-up joint account for a limited set of users of which I am included and that disclosure is limited to this set of users).

If I am given the details of a visitor account to pass on to my authorised visitor, this should not be disclosed to anyone other than my visitor.

I must not leave any computer unattended whilst logged on, nor interfere with others that are also logged on.

I must not borrow any ICT equipment without first seeking permission and signing it out with the ICT Support Team.

Data Protection/GDPR

I understand that:

- There are strict controls and requirements regarding the collection and use of personal data.
- The School has privacy notices that describe the collection and use of personal data.
- I will follow all requirements regarding Data Protection/GDPR.
- Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or governing body.
- Personal or sensitive data authorised to be taken off site must be encrypted.

- I must have permission from the school before making any recordings, images/photographs and videos. Adults should only use equipment provided or authorised by the school to make/take recordings, images/photographs and videos.
- Recordings, images and videos must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely.

Recordings, Images And Videos

Internet, mobile and digital technologies provide helpful recording functions, though these should only be used on equipment provided or authorised by the school.

Adults should only use equipment provided or authorised by the school to make/take recordings, images/photographs and videos. As soon as practicably possible, the resultant files from such recording or taking of photographs must be removed from any personal equipment used and stored in accordance with the school's procedures on school equipment.

I will not take images, sound recordings or videos of tuition or wider school events and activities on any equipment not provided or not authorised by the school.

When recording is authorised, school provided/authorised devices can be used for these purposes as long as there is agreement with the staff, student and parent/carer.

I will only upload images or videos of staff, students and/or parents/carers onto school approved sites where specific permission has been granted. The school's repository for recordings, images and videos is the R:\ drive.

Use Of Email

All such correspondence must be kept professional.

Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000 and/or GDPR subject access requests.

I will use my school provided email address or Governor Gateway for all school business. I will not use my school email addresses or Governor Gateway for personal matters or non-school business.

If I am not provided with a school email address because I am a temporary coach, visiting trainee or supply, then I will use my professional or formal university/college student email address for all school business. I will not use my professional email addresses for personal matters.

Sending/Uploading Personal/Sensitive Data

If I send personal/sensitive data via email, this should only be sent via password-protected attachments and the password sent under separate cover.

If I send personal/sensitive data via email internally, where possible I should avoid this and instead send a link to the location where information is stored on the school's network drives.

If I am required to upload data (ie: not sent via email), I will ensure that data is only uploaded to approved, known and secure websites (padlock symbol is visible).

Use Of Personal Devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of students. This therefore precludes the use of non-cloud based applications that store student data directly on personal devices. A school device could be used to access specialist apps that support student learning. Students can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carer agreement.

I will not access secure school information from personal devices unless permission has been given and the device is made sufficiently secure.

Additional Hardware/Software

I will not install any hardware or software on school equipment without permission of Network Support.

Promoting Online Safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, students and/or parents/carers) to the DSP and/or Network Support.

Classroom Management Of Internet Access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material that is visible (eg: adverts, other material and/or links to other material), however briefly, on the site. I will not free-surf the internet in front of students.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Network Support.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members), my company/organisations contract with the school (trainees/peripatetics/coaches/supply) and/or my responsibilities as a governor.

I have read and will follow the points made in "General Data Protection Regulation (GDPR) - TBSHS Do's and Don'ts".

Full Name:

Job Title/Role:

Signature:

Date:

| |
|--|
| |
| |
| |
| |

Appendix B - Requirements for Visitors, Volunteers and Parent/Carer helpers (Working directly with children or otherwise)

School Name: The Bishop's Stortford High School

Online Safety Coordinator: Assistant Headteacher with pastoral responsibility for Key Stage 4.


Designated Safeguarding Person (DSP): Wendy Butler

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the Headteacher and/or DSP

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to students and parent/carers. Where appropriate I may share my professional contact details with parents/carers provided the DSP or Headteacher is informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about students, staff, school systems and plans. Such information should never be shared online, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the Headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of students. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Appendix C - Students Years 07 to 11 - Internet/IT Equipment/Mobile Devices - Acceptable Use Agreement (Student and Parent/Carer)

| | | | | |
|--|---|---|----------------|------------------|
|  | <p>THE BISHOP'S STORTFORD HIGH SCHOOL London Road, Bishop's Stortford, Hertfordshire, CM23 3LU, UK. +44 1279 868686</p> | <p>Agreement Internet/IT Equipment/Mobile Devices - Acceptable Use (Yr07-11 Student and Parent/Carer)</p> | <p>S P</p> | <p>V20190916</p> |
|--|---|---|----------------|------------------|

Internet/IT Equipment/Mobile Devices - Acceptable Use Agreement (Student and Parent/Carer)

The internet, email, mobile technologies and online resources have become an important part of learning and life. The school want all students to be safe and responsible when using any IT. It is essential that students are aware of online risk, know how to stay safe and know where to go to report problems and access support.

Students are expected to read and discuss this agreement with their parent/carers and then to sign below as indicated and to follow the terms of the agreement.

The School's E-Safety, Internet Use and Data Security Policies have been drawn up to protect all parties - Students, Staff and the school. All students and staff using the IT equipment and Internet at the school must sign the Acceptable Use Agreement before access will be given. The network is owned by the school and access is given on the understanding that it is for educational use only.

All users need to understand that everything that they search for, access, post or receive online can be traced now and in the future. Their activity can be monitored and logged and if necessary shared with staff, parents/carers and/or the police.

Main Principles:

- All users of the internet are responsible for their behaviour and any communications sent over it;
- All users need to realise it is essential that they maintain a good online reputation and digital footprint;
- No activity shall be undertaken which could either threaten the integrity of the school ICT systems or attack or corrupt other systems;
- Only use school IT equipment for school purposes;
- Treat all equipment with respect;
- Access must only be made through authorised accounts;
- Users may not make purchases or enter into contracts over the Internet using school systems;
- Online chat is not permitted, either across the school network or over the internet;
- Students contacting teachers electronically, other than via the school e-mail system on a school related matter, is strictly forbidden;
- Posting anonymous messages and forwarding chain letters is not permitted;
- Use of the Internet to access inappropriate material such as pornographic, racist or offensive material is not permitted;
- Copyright of material must be respected.

I will:

- Only use school IT equipment for school purposes;
- Only log on to the school network, other school systems and resources using my own school user name and password;
- Be respectful to everyone online; treat everyone the way that I want to be treated. Ensure that all online activity, both inside and outside school, will not cause distress to anyone in the school community and bring the school into disrepute;
- Respect the privacy and ownership of others' work online and will adhere to copyright at all times;
- Make sure that all my electronic communications are responsible and sensible and couched in professional terms;
- Report any accidental infringement of these conditions to the ICT Support Team;
- Treat all equipment with respect;
- Leave the public work areas tidy;
- Ensure I have logged-out properly before leaving;
- Ensure equipment is shut down correctly and switched-off overnight.

I will not:

- Divulge my password to anyone other than a member of the school ICT Support Team;
- Allow any other person the use of a computer to which I have logged on to;
- Lie about my age in order to sign up for age inappropriate games, apps or social networks;
- Give out my own or any others' personal information, including name, phone number, home address, interests, schools or clubs or any personal image. (I will report immediately any request for any kind of personal information, to a member of staff if in school or a parent/carers if not in school);
- Use a personal email address or other personal accounts on school IT equipment;
- Upload any images, videos, sounds or words that could upset, now or in the future, any member of the school community, as this is cyberbullying;

- Post photographs, videos or livestream without the permission of all parties involved;
- Respond to hurtful behaviour online but will report it. I have the right to block and will say no to any inappropriate or upsetting request;
- Browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately, to a member of staff if I am in school or parent/carer if I am not in school;
- Attempt to bypass the internet filtering system in school;
- Assume that new technologies can be brought into school and will check with staff before bringing in any device;
- Leave the computer unattended whilst logged on, nor interfere with others that are also logged on;
- Download or install software on school IT equipment;
- Copy any software from any computer owned by the school;
- Delete any software from any computer owned by the school;
- Change the configuration of any computer owned by the school;
- Attempt to access any area that has been protected from me by way of restricted permissions or hidden directories, folders or files on any computer system owned by the school;
- Store undesirable material on any part of the system (offensive literature, pornographic images and the like);
- Attempt to repair any ICT equipment owned by the school;
- Borrow any ICT equipment without first seeking permission and signing it out with the ICT Support Team;
- Eat or drink near any equipment;
- Leave laptops or other portable equipment unattended and vulnerable to theft. Users must lock them away when unattended;
- Use the system for personal gain, for promoting political views or any form of personal advertising.

I understand that:

- Everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers/staff, parents/carers and/or the police. I know it is essential that I maintain a good online reputation and digital footprint;
- Not everything I see or hear online is true, accurate or genuine. I will also know that some people on the internet are not who they say they are and may have ulterior motives for assuming another identity that will put me at risk. I will avoid meeting people I only know on the internet;
- These rules are designed to keep me safe now and in the future. If I break the rules, teachers/staff will investigate, I may be disciplined and my parents/carers may be contacted. If I break the law the police may be informed.

Violations of the school's Internet Access Policy will result, in the first instance, in a temporary or permanent ban on its use.

Subsequent violations will result in serious disciplinary action being taken and for students this may lead to Permanent Exclusion for persistent offenders.

Where appropriate the Police or other authorities will be involved and criminal proceedings may be instigated.

Hand-Held Device/Mobile Telephone Policy, Years 07 to 11

The school's policy on hand-held devices/mobile telephones is that your son will keep his hand-held device/mobile telephone turned-off at all times during the school day, not be used in the playground or corridors and only to access it in the classroom if required as part of the learning, and only with permission from the teacher.

If a student in Years 07 to 11 uses his hand-held device/mobile telephone at any other time and for any other reason, it will be confiscated, taken to the school office, locked away for safe-keeping and a phone call made home informing the parent/carer of the confiscation. Where possible the phone-call is then followed-up with an email message.

If deemed necessary, the device content may be searched by a senior member of staff.

If a student uses their phone in school without permission, it will be confiscated for a week. If you would like it returned earlier, a parent may collect the device in person from the school Reception after the day of confiscation before 3.30pm. If there is a proven safe-guarding issue to have the phone returned earlier, please contact the school. If these times are inconvenient then you will need to make alternative arrangements by calling **01279 869552** or **01279 869549**.

Please note the school office, where the phones are held, is locked from 4pm Monday to Thursday and from 3.30pm on a Friday and therefore there is no access to the phone until the following morning.

Please can you reiterate to your son that it is totally inappropriate for him to use or have his hand-held device/mobile telephone switched on during school hours. Also, he will not be allowed to use it to contact home should he forget any equipment, as he needs to take responsibility for his belongings and accept the consequences should he be sanctioned.

Other Sanctions:

- Viewing inappropriate imagery/video/websites will result in an after-school detention with the subject teacher.
- Viewing inappropriate imagery/video/websites on more than one occasion will result in a Head of Year detention. Persistent failure to adhere to student protocols will result in an internal suspension/fixed term exclusion.
- Taking photographs or video footage of staff or students without permission may result in a fixed term exclusion, or in more serious cases may lead to permanent exclusion.
- Failure to allow a senior member of staff to inspect a device may result in a fixed-term exclusion.

I have read the conditions above and sign to show my agreement to them:

Name/Reg-Group Of Student:

Signature Of Student:

Date:

| |
|--|
| |
| |
| |

Name Of Parent/Carer:

Signature Of Parent/Carer:

Date:

| |
|--|
| |
| |
| |

Parent/Carer Agreement

I/we have discussed this agreement with my son, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our son.

I/we agree to support my son in full with the terms of this agreement.

I/we also agree not to share school related information or images online or to post material that may bring the school or any individual within it into disrepute, including on social media forums. [Rather than posting negative material online, any parent/carer, distressed or concerned about an aspect of school should make immediate contact with the school where the school can deal with the issue. Negative postings about the school would affect the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, students and parents.]

The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form, or which undermines the school staff.

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own children, unless there is a pre-specified agreement. I/we understand that when on school premises but not in a designated area where phones can be used, they must be switched off and out of sight.


Name Of Parent/Carer:

Signature Of Parent/Carer:

Date:

| |
|--|
| |
| |
| |

Appendix D - Students Years 12 to 13 - Internet/IT Equipment/Mobile Devices - Acceptable Use Agreement (Student and Parent/Carer)

| | | | | |
|--|--|---|----------------------|-----------|
|  | THE BISHOP'S STORTFORD HIGH SCHOOL London Road, Bishop's Stortford, Hertfordshire, CM23 3LU, UK. +44 1279 868686 | Agreement Internet/IT Equipment/Mobile Devices - Acceptable Use (Yr12-13 Student and Parent/Carer) | S P | V20190916 |
|--|--|---|----------------------|-----------|

Internet/IT Equipment/Mobile Devices - Acceptable Use Agreement (Student and Parent/Carer)

The internet, email, mobile technologies and online resources have become an important part of learning and life. The school want all students to be safe and responsible when using any IT. It is essential that students are aware of online risk, know how to stay safe and know where to go to report problems and access support.

Students are expected to read and discuss this agreement with their parent/carers and then to sign below as indicated and to follow the terms of the agreement.

The School's E-Safety, Internet Use and Data Security Policies have been drawn up to protect all parties - Students, Staff and the school. All students and staff using the IT equipment and Internet at the school must sign the Acceptable Use Agreement before access will be given. The network is owned by the school and access is given on the understanding that it is for educational use only.

All users need to understand that everything that they search for, access, post or receive online can be traced now and in the future. Their activity can be monitored and logged and if necessary shared with staff, parents/carers and/or the police.

Main Principles:

- All users of the internet are responsible for their behaviour and any communications sent over it;
- All users need to realise it is essential that they maintain a good online reputation and digital footprint;
- No activity shall be undertaken which could either threaten the integrity of the school ICT systems or attack or corrupt other systems;
- Only use school IT equipment for school purposes;
- Treat all equipment with respect;
- Access must only be made through authorised accounts;
- Users may not make purchases or enter into contracts over the Internet using school systems;
- Online chat is not permitted, either across the school network or over the internet;
- Students contacting teachers electronically, other than via the school e-mail system on a school related matter, is strictly forbidden;
- Posting anonymous messages and forwarding chain letters is not permitted;
- Use of the Internet to access inappropriate material such as pornographic, racist or offensive material is not permitted;
- Copyright of material must be respected.

I will:

- Only use school IT equipment for school purposes;
- Only log on to the school network, other school systems and resources using my own school user name and password;
- Be respectful to everyone online; treat everyone the way that I want to be treated. Ensure that all online activity, both inside and outside school, will not cause distress to anyone in the school community and bring the school into disrepute;
- Respect the privacy and ownership of others' work online and will adhere to copyright at all times;
- Make sure that all my electronic communications are responsible and sensible and couched in professional terms;
- Report any accidental infringement of these conditions to the ICT Support Team;
- Treat all equipment with respect;
- Leave the public work areas tidy;
- Ensure I have logged-out properly before leaving;
- Ensure equipment is shut down correctly and switched-off overnight.

I will not:

- Divulge my password to anyone other than a member of the school ICT Support Team;
- Allow any other person the use of a computer to which I have logged on to;
- Lie about my age in order to sign up for age inappropriate games, apps or social networks;
- Give out my own or any others' personal information, including name, phone number, home address, interests, schools or clubs or any personal image. (I will report immediately any request for any kind of personal information, to a member of staff if in school or a parent/carers if not in school);
- Use a personal email address or other personal accounts on school IT equipment;
- Upload any images, videos, sounds or words that could upset, now or in the future, any member of the school community, as this is cyberbullying;

- Post photographs, videos or livestream without the permission of all parties involved;
- Respond to hurtful behaviour online but will report it. I have the right to block and will say no to any inappropriate or upsetting request;
- Browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately, to a member of staff if I am in school or parent/carer if I am not in school;
- Attempt to bypass the internet filtering system in school;
- Assume that new technologies can be brought into school and will check with staff before bringing in any device;
- Leave the computer unattended whilst logged on, nor interfere with others that are also logged on;
- Download or install software on school IT equipment;
- Copy any software from any computer owned by the school;
- Delete any software from any computer owned by the school;
- Change the configuration of any computer owned by the school;
- Attempt to access any area that has been protected from me by way of restricted permissions or hidden directories, folders or files on any computer system owned by the school;
- Store undesirable material on any part of the system (offensive literature, pornographic images and the like);
- Attempt to repair any ICT equipment owned by the school;
- Borrow any ICT equipment without first seeking permission and signing it out with the ICT Support Team;
- Eat or drink near any equipment;
- Leave laptops or other portable equipment unattended and vulnerable to theft. Users must lock them away when unattended;
- Use the system for personal gain, for promoting political views or any form of personal advertising.

I understand that:

- Everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers/staff, parents/carers and/or the police. I know it is essential that I maintain a good online reputation and digital footprint;
- Not everything I see or hear online is true, accurate or genuine. I will also know that some people on the internet are not who they say they are and may have ulterior motives for assuming another identity that will put me at risk. I will avoid meeting people I only know on the internet;
- These rules are designed to keep me safe now and in the future. If I break the rules, teachers/staff will investigate, I may be disciplined and my parents/carers may be contacted. If I break the law the police may be informed.

Violations of the school's Internet Access Policy will result, in the first instance, in a temporary or permanent ban on its use.

Subsequent violations will result in serious disciplinary action being taken and for students this may lead to Permanent Exclusion for persistent offenders.

Where appropriate the Police or other authorities will be involved and criminal proceedings may be instigated.

Hand Held Device/Mobile Telephone Policy, Years 12 and 13:

In line with the school's policy for Years 7 to 11 and to avoid distraction from learning, Sixth Form students cannot use their hand-held device/mobile telephone during the school day in the corridors and outside areas. They can only access it in the classroom if required as part of the learning, and only with permission from the teacher. They are allowed to use them within the confines of the Sixth Form Centre but not for gaming or general social media during study periods. Mobile phones can only be used for homework and research purposes in the Library.

Failure to comply with this policy will result in confiscation of the hand-held device/mobile telephone. If deemed necessary the device content may be searched by a senior member of staff.

On the first occasion, if the confiscation is before lunch, the device will be taken to the Sixth Form office, locked away for safe-keeping and returned to the student at the end of the school day. If the phone is confiscated after lunch, the phone will be returned to the student at the end of the day and the student will be expected to hand their phone in the following day.

On the second occasion, the device will be confiscated during the school day every day for a week; the student will have to hand in their phone to the Sixth Form office at 8.30am and collect it at 3.30pm.

A further offence will result in complete confiscation of the phone during the school day for a half term. In this case, an email will be sent home informing the parent/carer of the confiscation.

There will be an automatic standards detention for failure to hand in the phone on any day.

Please note the Sixth Form office, where the phones are held, is locked from 4.15pm Monday to Thursday and from

3.30pm on a Friday and therefore there is no access to the phone until the following morning.

Other Sanctions:

- Viewing inappropriate imagery/video/websites will result in an after-school detention with the subject teacher.
- Viewing inappropriate imagery/video/websites on more than one occasion will result in a Head of Year detention. Persistent failure to adhere to student protocols will result in an internal suspension/fixed term exclusion.
- Taking photographs or video footage of staff or students without permission will result in a fixed term exclusion, or in more serious cases may lead to permanent exclusion.
- Failure to allow a senior member of staff to inspect a device will result in a fixed-term exclusion.

I have read the conditions above and sign to show my agreement to them:

Name/Reg-Group Of Student:

Signature Of Student:

Date:

Name Of Parent/Carer:

Signature Of Parent/Carer:

Date:

Parent/Carer Agreement

I/we have discussed this agreement with my son/daughter, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our son/daughter.

I/we agree to support my son/daughter in full with the terms of this agreement.

I/we also agree not to share school related information or images online or to post material that may bring the school or any individual within it into disrepute, including on social media forums. [Rather than posting negative material online, any parent/carer, distressed or concerned about an aspect of school should make immediate contact with the school where the school can deal with the issue. Negative postings about the school would affect the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, students and parents.]

The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form, or which undermines the school staff.

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises but not in a designated area where phones can be used, they must be switched off and out of sight.

Name Of Parent/Carer:

Signature Of Parent/Carer:

Date:

Appendix E - Online safety policy guide - Summary of key parent/carers responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for students.
- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carers is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Parents/carers should not assume that students can bring technological devices to school and should always check the school policy.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.
- Any parent/carers, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, students and parents/carers.

Please see the full online safety policy in the policies section on the school website.

Appendix F - Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Students should report to a member of staff (e.g. class teacher, Head of Year) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the DSP so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix G - Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix E (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a student are of a serious nature, these will need to be formally investigated. This may involve the police and the Headteacher will need to follow the school's safeguarding procedures.

If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

Appendix H - Online safety incident reporting form

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident, please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to the Pastoral Deputy Headteacher.

| | | | |
|------------------------------------|----------------|--|-----------------|
| Name of person reporting incident: | | | |
| Signature: | | | |
| Date you are completing this form: | | | |
| Where did the incident take place: | Inside school? | | Outside school? |
| Date of incident(s): | | | |
| Time of incident(s): | | | |

| Who was involved in the incident(s)? | Full names and/or contact details |
|--------------------------------------|-----------------------------------|
| Children/young people | |
| Staff member(s) | |
| Parent(s)/carer(s) | |
| Other, please specify | |

| Type of incident(s) (indicate as many as apply) | | | |
|---|--|---|--|
| Accessing age inappropriate websites, apps and social media | | Accessing someone else's account without permission | |
| Forwarding/spreading chain messages or threatening material | | Posting images without permission of all involved | |
| Online bullying or harassment (cyber bullying) | | Posting material that will bring an individual or the school into disrepute | |
| Racist, sexist, homophobic, religious or other hate material | | Online gambling | |
| Sexting/Child abuse images | | Deliberately bypassing security | |
| Grooming | | Hacking or spreading viruses | |
| Accessing, sharing or creating pornographic images and media | | Accessing and/or sharing terrorist material | |
| Accessing, sharing or creating violent images and media | | Drug/bomb making material | |
| Creating an account in someone else's name to bring them into disrepute | | Breaching copyright regulations | |
| Other breach of acceptable use agreement, please specify | | | |

| | |
|----------------------------------|-------------------------|
| Full description of the incident | What, when, where, how? |
|----------------------------------|-------------------------|

| | |
|--------------------------------|---|
| Name all social media involved | Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc |
| Evidence of the incident | Specify any evidence available but do not attach. |

Thank you for completing and submitting this form.

Appendix I - Online safety incident record

| | | | |
|------------------------------------|----------------|--|-----------------|
| Name of person reporting incident: | | | |
| Date of report: | | | |
| Where did the incident take place: | Inside school? | | Outside school? |
| Date of incident(s): | | | |
| Time of incident(s): | | | |

| Who was involved in the incident(s)? | Full names and/or contact details |
|--------------------------------------|-----------------------------------|
| Children/young person | |
| Staff member(s) | |
| Parent(s)/carer(s) | |
| Other, please specify | |

| Type of incident(s) (indicate as many as apply) | | | |
|---|--|---|--|
| Accessing age inappropriate websites, apps and social media | | Accessing someone else's account without permission | |
| Forwarding/spreading chain messages or threatening material | | Posting images without permission of all involved | |
| Online bullying or harassment (cyberbullying) | | Posting material that will bring an individual or the school into disrepute | |
| Racist, sexist, homophobic, religious or other hate material | | Online gambling | |
| Sexting/Child abuse images | | Deliberately bypassing security | |
| Grooming | | Hacking or spreading viruses | |
| Accessing, sharing or creating pornographic images and media | | Accessing and/or sharing terrorist material | |
| Accessing, sharing or creating violent images and media | | Drug/bomb making material | |
| Creating an account in someone else's name to bring them into disrepute | | Breaching copyright regulations | |
| Other breach of Acceptable Use Agreement | | | |
| Other, please specify | | | |

| | |
|----------------------------------|-------------------------|
| Full description of the incident | What, when, where, how? |
|----------------------------------|-------------------------|

| | |
|--------------------------------|---|
| Name all social media involved | Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc |
| Evidence of the incident | Specify any evidence provided but do not attach |

| Immediate action taken following the reported incident: | |
|--|--|
| Incident reported to online safety Coordinator/DSP/DSP/Headteacher | |
| Safeguarding advice sought, please specify | |
| Referral made to HCC Safeguarding | |
| Incident reported to police and/or CEOP | |
| Online safety policy to be reviewed/amended | |
| Parent(s)/carer(s) informed please specify | |
| Incident reported to social networking site | |
| Other actions e.g. warnings, sanctions, debrief and support | |
| Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery | |

| | |
|---|--|
| Brief summary of incident, investigation and outcome (for monitoring purposes) | |
|---|--|

Appendix J - Online safety incident log

Summary details of ALL online safety incidents will be recorded on this form by the online safety coordinator or other designated member of staff. This incident log will be monitored at least termly and information reported to SLT and governors.

| Date & time | Name of student or staff member Indicate target (T) or offender (O) | Nature of incident(s) | Details of incident (including evidence) | Outcome including action taken |
|-------------|--|-----------------------|--|--------------------------------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |