BISHOP STOPFORD'S SCHOOL

Online Safety Policy

Drafted by:	Garry Lyle, Deputy Headteacher in February, 2020
Approved by the Governing Body:	23rd February, 2022
Date of next review:	February, 2023

Contents

1. Aims

Bishop Stopford's School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education – remove if not applicable, see section 4]
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The Governing Body may also if required co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's DSL and other safeguarding officers are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, Network Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher

3.4 The Network Manager

The Network Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.6 Parents and Carers

Parents and Carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All secondary schools will have to teach 'Relationships and sex education' and 'health education.' This new requirement includes aspects about online safety.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

The safe use of social media and the internet will also be covered in other subjects where relevant and we will use assemblies and curriculum drop-down days where appropriate to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents and carers about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This online safety policy will also be shared with parents and carers.

Online safety will also be covered where appropriate during parents' evenings.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also ensures our website has links to invaluable information and advice on cyber-bullying to parents and carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Bishop Stopford's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school’s internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school but are not permitted to use them (unless instructed to do so by members of staff). This includes:

- Lessons
- Form time
- Break and Lunch times
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device for a fixed period of time before being returned to parents/carers.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school’s terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Network manager or DSL.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school’s ICT systems or internet, we will follow the procedures set out in our acceptable use policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet; or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct and acceptable use policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and safeguarding officers will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed every two years by the Deputy Headteacher. At every review, the policy will be shared with the Governing Body.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use policies

Appendix 1: Acceptable use agreement (pupils and parents/carers)

When using the school's ICT systems (like computers, Google Classroom) and get onto the internet in school:

1. I will only use ICT systems in School, including the Internet, e-mail, digital video and mobile technologies for School purposes.
2. I will not download or install software on School technologies.
3. I will only log on to the School network, other systems and resources with my own user name and password.
4. I will follow the Schools ICT security system by setting secure passwords, not reveal them and change them regularly.
5. I will disable cellular internet connection whilst in School on any device and connect to the internet only through the School wireless system.
6. I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
7. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
8. I will not access or attempt to access accounts belonging to other users.
9. I will not deliberately browse, download, upload or forward material that could be considered or illegal. If I accidentally come across any such material I will report it immediately.
10. Images of pupils and/or staff will only be taken, stored and used for School purposes in line with School policy and not distributed outside the School network without the permission of the Headmaster.
11. I will follow guidance and advice to ensure I use the Internet and related digital technologies safely. I will not give out personal information such as name, address or phone number. If I am concerned about mine, or someone else's, safety online I will speak to an adult.
12. I will ensure that my online activity, both in School and outside School, will not cause my School, the staff, pupils or others distress or bring into disrepute.
13. I will support the School approach to online safety and not deliberately upload or add any images, video, sounds, or text that could upset any member of the School community.
14. I will respect the privacy and ownership of others work on-line at all times. This includes respecting all copyright laws and never knowingly plagiarising another person's work.
15. I will not attempt to bypass the Internet filtering system.
16. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to teachers.
17. I understand that these rules are designed to keep me safe and that if they are not followed, School sanctions will be applied and my parent/carer may be contacted.
18. I will tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others and understand that I can contact the ThinkUKnow website to report this material as well.
19. I will not arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
20. I understand that personal mobile phones or other personal electronic devices are not to be used in school unless instructed to do so by a member of staff and that they may be confiscated if seen or being used without permission.

https://www.thinkuknow.co.uk/

http://www.ceop.police.uk/Safety-Centre/

To report abuse click on or type in this link.

Appendix 2: acceptable use agreement (governors, volunteers and visitors)

ICT and related technologies such as e-mail, the Internet and mobile devices are an expected part of our daily working life in School. The policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

Any concerns or clarification should be discussed with the Designated Safeguarding Lead Officer. Staff should be aware that a breach of this acceptable use policy may amount to misconduct and result in disciplinary proceedings.

When using the school's ICT systems (like computers, Google Classroom) and get onto the internet in school:

1. I will only use the Schools email/Internet/Intranet/learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
2. I will limit the use of the internet for personal use to out of lesson time for teaching staff and to breaks and lunchtime for support staff.
3. I will confine my use of my personal mobile phone to private staff areas only.
4. I will comply with the ICT system security and ensure that I keep my password secure and ensure staff pages cannot be accessed by pupils by not leaving an unattended computer logged on and unlocked or let Students access it.
5. I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
6. I will not give out my personal details, such as mobile phone number and personal email address, to pupils.
7. I will ensure that any personal data (such as data held on BROMCOM) is kept secure and is used appropriately, whether in School, taken off the School premises or accessed remotely at home.
8. I will not install any hardware or software to School devices without the permission of IT services.
9. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
10. Images of pupils and/or staff will only be taken, stored and used for professional purposes and with the written consent of parent, carer or member of staff. (A list of pupils who cannot be photographed for publicity purposes is held in the School Office).
11. I will not use my own mobile phone to record images of pupils. School cameras are available for recording such images. I will not download images of pupils to my own personal devices.
12. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
13. I will support the School approach to e-safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the School community.
14. I will respect copyright and intellectual property rights.
15. I will ensure that my online activity, both in School and outside School, will not bring my professional role into disrepute.
16. I will support and promote the School's e-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
17. I will not accept any current pupil of any age or any ex-pupil of the School under the age of 21 as a friend, follower, subscriber or similar on any personal social media account, including any form of on-line gaming.
18. I will only use School sanctioned social media accounts for the communicating of official School business or news.
19. I will let the designated safeguarding lead (DSL) and Network Manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
20. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Appendix 3: online safety training needs – self audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: online safety incident report log

<table>
<tr><th colspan="5">Online safety incident log</th></tr>
<tr><th>Date</th><th>Where the incident took place</th><th>Description of the incident</th><th>Action taken</th><th>Name and signature of staff member recording the incident</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>