BISHOP VESEY'S GRAMMAR SCHOOL
Online Safety Policy

Staff covered by this procedure:	Teaching and support staff
Review prepared by:	Designated Safeguarding Lead – Kate Steadman
Reviewed by and date:	Headteacher December 2019
Signed by Headteacher	
Date of Next Review/by whom	Full Board of Governors Autumn 2022

ONLINE SAFETY POLICY

1. Introduction

1.1 This policy applies to all members of Bishop Vesey's Grammar School who have access to and are users of school digital technology systems, both in and out of the school.

1.2 The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

1.3 The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that takes place out of school.

2. Roles and Responsibilities

Governors

2.1 Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor (it is suggested that the role may be combined with that of the Child Protection / Safeguarding Governor).

2.2 The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / Committee / meeting

The Head Teacher:

2.3 The Head Teacher, Mr Dominic Robson, has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Officer, Assistant Head Teacher Kate Steadman.

2.4 The Head Teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

2.5 The Head Teacher is responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

2.6 The Head Teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety-monitoring role. This is to

provide a safety net and support to those colleagues who take on important monitoring roles.

The Online Safety Officer

2.7 The Online Safety Officer is responsible for:

- taking day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- providing training and advice for staff
- liaising with school technical staff
- receiving reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meeting with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs

The Network Manager

2.8 The Network Manager is responsible for ensuring:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets required online safety technical requirements and any Local Authority Online Safety Policy that may apply.
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher Online Safety Officer or investigation / action / sanction
- monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Non-Teaching Staff

2.9 Teachers and non-teaching staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current *school* Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy

- they report any suspected misuse or problem to the *Headteacher , Online Safety Officer, Heads of Year* for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices

Students

2.10 Students are responsible for ensuring that:

- they use the digital technology systems in accordance with the Student Acceptable Use Agreement
- they have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- they know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- they understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents and Carers:

2.11 Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the *school* in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line student / pupil records

3. Policy Statements

Education- Students

3.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

3.2 Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of
- assemblies and tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Education- Staff

3.3 Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

3.4 In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

3.5 Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

3.6 It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

4. Technical- Infrastructure/equipment, filtering and monitoring

4.1 The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this

policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the ICT team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.

4.2 The administrator passwords for the school ICT systems, used by the Network Manager must also be available to the Head Teacher and kept in a secure place

4.3 The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

4.4 Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored

4.5 Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.

4.6 Appropriate security measures are in to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

5. Mobile Devices- BYOD

5.1 Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

5.2 All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy is consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage.

5.3 Please see the Mobile Devices policy for further information and detail.

6. Use of digital and video images:

6.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

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

6.3 Written permission from parents or carers will be obtained before photographs of students are published on the school website / social media / local press

6.4 In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students* in the digital / video images.

6.5 Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school / academy equipment, the personal equipment of staff should not be used for such purposes.

6.6 Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school / academy into disrepute.

6.7 Students must not take, use, share, publish or distribute images of others without their permission.

6.8 Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

6.9 Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6.10 Student's work can only be published with the permission of the student and parents or carers.

7. Data Protection

7.1 Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

7.2 The school has a Data Protection policy and it has appointed a Data Protection Officer, Mr Graham Swindells.

7.3 The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

7.4 Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.

7.5 The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.

7.6 Where special category data is processed, a lawful basis and a separate condition for processing have been identified.

7.7 Data Protection Impact Assessments are carried out.

7.8 The school has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.

7.9 Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.

7.10 There are clear and understood data retention policies and routines for the deletion and disposal of data.

7.11 There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.

7.12 Consideration has been given to the protection of personal data when accessed using any remote access solutions.

7.13 Bishop Vesey's has a Freedom of Information Policy which sets out how it will deal with FOI requests.

7.14 All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

7.15 Staff must ensure that they:
At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

7.16 Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

7.17 Transfer data using encryption and secure password protected devices.

7.17 When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school / academy policy (below) once it has been transferred or its use is complete.

8. Communication

8.1 When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

9. Social Media Protecting Professional Identity

9.1 All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

9.2 The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

9.3 School staff should ensure that:

- No reference should be made in social media to students, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community

- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

9.4 When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including:
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school / academy disciplinary procedures

10. Personal Use

10.1 Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

10.2 Personal communications which do not refer to or impact upon the school are outside the scope of this policy

10.3 Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

11. Monitoring of Public Social Media

11.1 As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school

11.2 The school should effectively respond to social media comments made by others according to a defined policy or process

11.3 The school*'s* use of social media for professional purposes will be checked regularly by the Online Safety Officer to ensure compliance with the school policies

12. Dealing with unsuitable/inappropriate activities

12.1 Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other technical systems. Other activities e.g. cyber-bullying are banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

12.2 The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	

Illegal Incidents:

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.