Unity Schools Trust

'Excellence through collaboration'

Bishop David Brown School

On-Line Safety Policy

Policy Reviewed:	June 2020
Next Review:	June 2021
Approved by Local Governing Body	September 2020

Contents

1. Aims

At Bishop David Brown School, we encourage student engagement with Information Technology (IT) as we believe that it enables them to learn, communicate and explore the world in new ways. Many young people are now skilled in using computers, games consoles, mobile phones and tablet computers. However, with this new technology we also acknowledge that there are also new risks.

We believe that everyone in our school community is responsible for the welfare and safety of children and it is therefore crucial that all stakeholders understand what these risks are and how we can all work together to enjoy these new technologies safely.

E-Safety is essentially about creating a safe environment when using IT. This includes the use of the internet and social networking sites. This document is intended to outline the school's approach to preventing safeguarding issues, including cyber bullying, as well as detailing how we respond to e-safety issues when they emerge.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the internet and other digital technologies. Indeed, some young people may find themselves".

Safeguarding Children in a Digital World – Becta ICT Advice

Our aim is to address these potential issues by regularly providing clear guidelines and information to students, their parents and staff about how to keep young people safe and by dealing rapidly with any emerging concerns through a consistent approach, as outlined in this document; this will invariably involve close communication with parents and where necessary, liaison with Children's Services, the Police and other relevant agencies.

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
- Searching, screening and confiscation

It also refers to the Department'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.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governors who oversee online safety are George Pincus and Clair Davies.

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 IT systems and the internet.

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 deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.

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, IT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The Network manager

The IT 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 IT 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 IT 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 and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

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 IT 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 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

This list is not intended to be exhaustive.

3.6 Parents

Parents 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 IT systems and internet.

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 factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT 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.

4. Educating pupils about online safety

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

From September 2020 **all** schools will have to teach:

- Relationships and sex education and health education in secondary schools and 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.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

The Child Exploitation and Online Protection Centre (CEOP, http://www.ceop.police.uk/) brings together law enforcement officers and specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24 hour online facility for reporting instances of online child sexual abuse. CEOP's 'Report Abuse' button is on the home page of our school's website and every year students are informed of how to use this facility to report online abuse.

All students receive discrete lessons on Internet Safety in the first few weeks of school. Years 7, 8 and 9 also complete badges in eSafety, Digital Ethics, Social Media Ethics, Safe Online, as well as Fake News and Cyber Security using the iDEA website.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents.

Online safety will also be covered during parent information evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or 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. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

All staff at Bishop David Brown School are aware of the need to be alert to cyber bullying and in line with our Behaviour and Anti Bullying Policy, staff are expected to report all instances of bullying, including racist and homophobic bullying, to a member of the pastoral team, who will address these issues as a matter of urgency. More serious cases of bullying or ongoing bullying following intervention should be discussed with the school's DSL/DDSL and could involve making a referral to Children's Services. Separate referrals for assessment and support may be made in respect of both child victim and child abuser.

Where the bullying involves an allegation of crime (threats of assault, theft, harassment) a referral may be made to the police. Information about good practice in anti-bullying strategies (real & virtual) for schools, can be accessed at;

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/623895/Preventing_and_tackling_bullying_advice.pdf

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 Child Exploitation and Online Protection Centre (CEOP, http://www.ceop.police.uk/) brings together law enforcement officers and specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24 hour online facility for reporting instances of online child sexual abuse. CEOP's 'Report Abuse' button is on the home page of our school's website and every year students are informed of how to use this facility to report online abuse.

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 sends information/leaflets on cyber-bullying to parents 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.

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 IT systems and the internet. 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.

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Break 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.

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.

8. 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.

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 IT manager.

Work devices must be used solely for work activities.

For further information, please see the IT and internet acceptable use policy.

9. Social Media

This policy sets out the procedures and ideals for all staff members of Bishop David Brown, are expected to follow when using social media. The policy is to be followed to ensure that students, staff and the school reputation are protected.

This policy is intended to cover social media used for official school purposes, including those hosted by the school, as well as personal social media sites where the school is directly named or referred to.

Social media sites include, but are not restricted to, networking sites, blogs, chatrooms or forums, and content sharing sites.

Ideals:

- Staff should at all times be conscious of keeping their personal and work life separate and should not put themselves in a position of conflict between themselves and Bishop David Brown School on social media.
- Staff should not be using social media in such a way that Bishop David Brown School is viewed or judged in a negative manner.
- Social media must not be used to insult or defame staff, students, or associates linked to an individual known to the staff member through Bishop David Brown School, on any social media site.
- Personal views of staff should not be represented as the views of Bishop David Brown School.

- Staff should not be discussing or sharing personal information about staff, students or associates linked to them through BDB on any social media site.
- Staff should always try to be accurate, positive and fair when creating or amending social media information in the name of Bishop David Brown School.
- Staff should not share or upload information that identifies students by their full name unless written permission has been granted by the parent/ carer/ guardian.
- Staff should always follow the school policy with regards students whose picture and name are not to be used in a public forum when using social media.
- Staff must at all times act in a positive manner and with the best interest of BDB in mind when sharing information about BDB on social media.

For further information, please see the IT and internet acceptable use policy.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our behaviour policy. 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 IT 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

All members of our school community should be aware of their responsibility to follow safeguarding procedures if they have a concern that adult staff members or volunteers may be accessing indecent images of children. Employees of the school are regularly made aware of the Whistleblowing Policy and the headteacher must follow Surrey's Safeguarding Children's Board interagency procedures in dealing with such allegations. The Local Authority Designated Officer (LADO) holds the responsibility for ensuring that allegations against members of staff are properly investigated. Bishop David Brown School follows LADO procedures in all cases where it is alleged that a person who works with children has:

- behaved in a way that has harmed a child, or may have harmed a child;
- possibly committed a criminal offence against or in relation to a child;
- behaved toward a child or children in a way that indicates she or he is unsuitable to work with children.

In operating the LADO procedures the school must consider whether the allegation can be properly investigated if the person concerned remains in work. Schools can seek advice about suspension and alternatives to suspension but the final decision remains with the school. It would be very unusual for the school not to take the advice of the LADO and if it were to do so, the LADO may decide to take the issue to the education secretary.

It is important that individuals suspected of accessing, creating or downloading indecent images of children are not alerted prior to the police undertaking their investigations as they may destroy computer evidence at work or home. This has implications for managing allegations against people who work with children and means individuals may not initially be fully informed of reasons for their suspension.

Research into investigations of adults accessing child abuse images has identified that professional staff accessing such images may have access to children both in their

occupation and in their personal lives. In such cases, a section 47 strategy discussion (Children Act 1989) will consider the need to assess risk both in relation to the occupation and in relation to the risk to any child within the family of the individual concerned. The Head of School and/or the DSL will be involved in this strategy meeting.

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 their deputies 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

User logins, user printing, user door access, internet access and inappropriate activity on PCs and laptops are all monitored and reported to the appropriate school leader if concerns arise.

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every two years by the governing body. At every review, the policy will be shared with the governing board.

13. Systems and Procedures

Procedures are in place to protect the school and its students from a malicious cyber-attack. All computer equipment is protected by the security of the school. All external doors to buildings are locked. Visitors to the site are booked in. Servers, PBX and network storage are kept in locked rooms with restricted access. Network communications equipment is kept in locked cabinets. The school network is protected behind the RM SafetyNet to protect from external malicious attack.

Access to Servers and Network is limited to a few school technical staff. Individual user ids are used and are protected with strong passwords. Any attempt internally at unauthorised access to servers is logged by the forensic software. All user data is backed up daily. Critical servers are backed up weekly.

The school uses VLANs to separate curriculum and administration networks, restricting activity and access as appropriate.

In order to prevent unauthorised users downloading software on school devices, laptops and desktop PCs are protected by user names and passwords. Students are automatically

blocked from downloading software and virus guards are installed so that staff who download software can do so safely.

Access to school networks and devices is controlled through careful password procedures, whereby students are taught about password strengths in their IT lessons, before setting strong passwords of six characters which include upper and lower case letters as well as either a symbol or a number. Additionally, each user has a home folder on the server which cannot be accessed by other users. Students and staff also have access to their own designated shared areas which contain resources. Staff can also access students' home folders.

School IT induction for staff ensures that they are briefed on the dangers of viruses and attachments. Emails are regularly sent out reminding staff of the need to be vigilant.

Bishop David Brown School is cautious in using external internet services and as such, for third party vendors, it is required that any internet access for students is only provided through the school's internet filter and forensic software.

Procedures are in place to provide internet access to temporary staff such as trainee teachers, through temporary user IDs. Guest wifi is also being developed to allow guest access to the internet but not the local school network.

Bishop David Brown uses 'RM SafetyNet', a Firewall software package, to filter internet content. This is run on a proxy in school. All internet traffic goes out through the school RM SafetyNet so is filtered and monitored.

PCE software provides a forensic logging ability and inappropriate use or attempt is logged. These logs are actively monitored. The logging also applies to staff but is not actively reviewed.

Students are limited by blocking lists which restrict content. However different levels of blocking can be applied to different year groups. This is done on a request basis, linked to curriculum needs.

Students and staff who attempt to access a blocked site are informed by a RM SafetyNet screen message. Additionally, the Acceptable Use Agreement includes statements on logging and monitoring of school IT equipment. Should a member of staff require the temporary lifting of a website restriction they are required to inform the IT helpline in school and the information is logged. The log contains the following details: the name of the member of staff, the date, the URL, the reason, the reversion date, the person making the change, the year groups or staff using the site

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices

- Staff code of conduct
- Complaints procedure
- IT and internet acceptable use
- Staff code of conduct

Appendix 1: Acceptable use agreement for pupils

Acceptable use of the school's IT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
I appreciate that IT includes a range of systems, including mobile phones, cameras, email, social networking, laptops and personal devices used for school activities. **When using the school's IT facilities and accessing the internet in school, I will not:** • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break school rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the school's network using someone else's details- I understand that I am responsible for all activity carried out under my username. • Bully other people • Install hardware or software without permission form the network manager. • Browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. I understand that the school will monitor the websites I visit and my use of the school's IT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's IT systems and internet responsibly. I will ensure that my online activities, both in school and outside school, will not bring the school into disrepute. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

I appreciate that IT includes a range of systems, including mobile phones, cameras, email, social networking, laptops and personal devices used for school activities.

When using the school's IT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- Browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

I understand that the school will monitor the websites I visit and my use of the school's IT facilities and systems.

I will only use approved, secure email systems for any school business.

I will ensure that data (such as that held in SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the head teacher.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and IT 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.

I will always use the school's IT systems and internet responsibly, and ensure that pupils in my care do so too.

I understand that all of why use of the internet and other related technologies can be monitored and logged and can be made available, upon request, to my line manager or head teacher.

Images of pupils and/ or staff will only be taken, stored and sued for professional purposes in line with school policy and with written consent of the parent/ carer or staff member.	
Signed (staff member/governor/volunteer/visitor):	**Date:**