BISHOP STOPFORD'S SCHOOL

E – Safety Policy

Drafted by:	Pinar Erol, E-Safety designated safeguarding officer
Approved by the Governing Body:	February, 2018
Date of next review:	February, 2019
Person to initiate review:	Headteacher
Document file name:	Online Safety Policy BSS 2017

Contents

Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Bishop Stopford's School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of the Bishop Stopford's School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the school's IT systems, both in and out of Bishop Stopford's School.

Roles and responsibilities Role	Key Responsibilities
Head Teacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident (see A4) • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To ensure the Safeguarding Team regularly monitor online safety. • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.

Jonathan Seabrook, Lead Designate - Senior AHT Shereka James, DHT – Deputy DSL Tammy Day, Head Teacher Ella Moynihan – AHT Michelle Effah-Damoah - AHT Alfie Egembah – AHT Peter Smyth -Head of Year 7 Christina Morgan - Head of Year 8 Maria Pavlou - Head of Year 9 Tracy Dorrington - Head of Year 10 Robert Smith - Head of Year 12 & 13 Emma Lee-Ince - Head of PE Department Tamsin Holland -Head of PE Department Carol Hart - SENCO Pinar Erol - Head of ICT & Business Department Eva Budweg - EAL Teacher Abdul Basith - Business and ICT Teacher Judith Dougherty – Head of Performing Arts – Teacher Governor	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the
Safeguarding Governor	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • To regularly monitor the safeguarding team with regards to online safety.
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/technician	• To report online safety related issues that come to their attention, to the Safeguarding Team • To manage the school's computer systems, ensuring - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant

	• That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures.
Data and Information (Admin Team)	• To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant.
Teachers	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff (incl. club staff) and students.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction. • To report any suspected misuse or problem to the Safeguarding Team. • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology Exit strategy • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and 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 • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child(ren) • To consult with the school if they have any concerns about their child(ren)'s use of technology • To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • To support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and shared ‘W’ drive.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year.

Acceptable use agreements to be issued to whole school community, on entry to the school. Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- The Safeguarding Team acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to the Safeguarding Team that day.
- Any concern about staff misuse is always referred directly to the Head Teacher, unless the concern is about the Head Teacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority’s Designated Officer).

“Review and monitoring the online safety policy” is referenced within other school policies (e.g. Safeguarding, Anti-Bullying policy, PSHE, Computing policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

Education and Curriculum Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum and other curriculum areas as relevant.

This covers a range of skills and behaviours appropriate to their age and experience;

- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;

- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;

- ensure, whilst at school, pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training - this school

- makes regular training available to staff on online safety issues and the school's online safety education program;

Parent awareness and training - this school

- provides information in the induction pack for parents which includes online safety;

- runs a rolling programme of online safety advice, guidance and training for parents, with the support of the PTA.

Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;

- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;

- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;

- understand the importance of adopting good online safety practice when using digital technologies in and out of school;

- know and understand school policies on the use of mobile and hand held devices including cameras (see below);

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;

- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;

- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse

Incident Management In this school

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;

- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;

- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, Internet Watch Foundation) in dealing with online safety issues;

- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;

- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;

- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;

- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

Managing IT and Communication System Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;

- has the educational filtered secure broadband connectivity through the LGfL;

- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming).

All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;

- uses USO user-level filtering where relevant;

- ensures network health through use of Sophos anti-virus software (from LGfL);

- Uses DfE, LA or LGfL approved systems such as LGfL USO FX2 to send 'protect-level' (sensitive personal) data to external agencies over the Internet

- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;

- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

This school:

- Uses individual, audited log-ins for all users - the LGfL USO system;

- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;

- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;

- Has additional local network monitoring/auditing software installed;

- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;

- Has daily back-up of school data (admin and curriculum);

- Uses secure, data back-up that conforms to DfE guidance;

- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access.

Online access to service is through a unique, audited username and password. We also provide a different username and password for access to our school's network;

- All pupils have their own unique username and password which gives them access to the Internet and other services;

- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;

- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;

- Requires all users to log off when they have finished working;

- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;

- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.

- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.

- Maintains equipment to ensure Health and Safety is followed;

- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:

Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited, restricted and is only through approved systems;

- Has a clear disaster recovery system in place that includes a secure, remote off site back up of cloud data and the safe storage of data in a fireproof safe;

- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;

- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);

- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;

- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards; Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others. If a password is compromised the school should be notified immediately.

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.

- We require staff to use STRONG passwords.

- We require staff to change their passwords into the MIS, LGfL USO admin site, if we have reason to believe that safety may be compromised.

- We require staff using critical systems to use two factor authentication.

- Supply teachers have their own password which only allows access to the Curriculum folder on the W drive. E-mail This school

- Provides staff with an email account for their professional use - London Staffmail - and makes clear personal email should be through a separate account;

- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

- Will ensure that email accounts are maintained and up to date

- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses. Pupils:

- We use the LGfL pupil email system which are intentionally 'anonymised' for pupil protection.

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff will use LGfL e-mail systems for professional purposes

- Access in school to external personal e mail accounts may be blocked.

- Never use personal email to send staff or pupil personal data. School website

- The Head Teacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

- The school web site complies with statutory DFE requirements;

- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;

- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website; Cloud Environments

- Uploading of information on the school's online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas and pupils upload to their own approved areas using accounts provided by the school.

- Photographs and videos are uploaded to either the school’s online environment or approved accounts and will only be accessible by members of the school teaching staff and or the individual pupil.

- In school, pupils are only able to upload and publish within school approved ‘Cloud’ systems.

From home, pupils and parents/guardians will be able to access the pupils' approved OneDrive accounts with authentication.

Social networking Staff (including club staff), Governors and Students

- Staff (including club staff), Governors and Students are instructed to always keep professional communication away from public social networks.

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their pupils, but to use the schools’ preferred system for such communications.

- The use of any school approved social networking will adhere to Safer Working Practice.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents or carers in context of school activities.

No social media posts should be made that compromises the professional role or image of a staff member.

- School staff should not be online friends with any pupil.

Any exceptions must be approved by the Head Teacher.

- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute. • Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse at an age-appropriate level through our online safety curriculum work.

- Students are required to sign and follow our age appropriate pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.

- We ask parents not to upload any photos of their children from a school event onto a public social media site.

Recording Equipment

- We use recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Data security

Management Information System access and Data transfer Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).

- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.

- We ensure staff know to whom to report any incidents where data protection may have been compromised.

- All staff are DBS checked and records are held in a single central record Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.

- We require staff to lock their workstation when leaving their computer for a prolonged period of time. The system will enforce a lock-out after 30 minutes idle time.

- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.

- All servers are in lockable locations and managed by DBS-checked staff.

- Details of all school-owned hardware will be recorded in a hardware inventory.

- Details of all school-owned software will be recorded in a software inventory.

- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

- We are using secure file deletion software when retiring a machine.

Equipment and Digital Content Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

- All mobile devices brought in to school by a pupil will be turned off and handed in at the school office at the start of the day. They then collect their device at the end of the school day.

- Personal mobile devices will not be used by staff during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.

- All visitors are requested to keep their phones on silent.

- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.

- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

- Staff may use their phones during break times or during non-contact times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions from their line manager to use their phone at other times. Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.

- PIN access to the device must always be known by the network manager. The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.

- PIN access to the device must always be known by the network manager.

- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Students’ use of personal devices

- The School strongly advises that student mobile phones and devices should not be brought into school.

- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.

- Phones and devices must not be taken into examinations. Students found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student’s withdrawal from either that examination or all examinations.

- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

- Students will be provided with school mobile devices to use in specific learning activities under the supervision of a member of staff. Such mobile devices will be set up so that only those features required for the activity will be enabled. Staff use of personal devices

- Staff are only permitted to use their own mobile phones or devices in a professional capacity, (such as for contacting children, or their families within or outside of the setting) if no school phone is available.

- If members of staff have an educational reason to allow children to use personal mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.

- No images, videos or recordings should be taken of pupils on personal mobile devices at school or on official school activities. Any exceptions must be explicitly authorised by the Head Teacher.

- In an emergency where a staff member doesn’t have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes

- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this school:

• We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school

• We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;

• Staff sign the school's Acceptable Use Policy which covers the use of personal mobile devices for taking pictures of pupils;

• The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;

• Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;

• Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

• Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Radicalisation and Extremism

The school's safeguarding policy which is available on our website, covers Radicalisation and Extremism

Indicators of Vulnerability to Extremism and Radicalisation

Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

Extremism is defined by the Government in the Prevent Strategy as:

- Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs.

- We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas.

Extremism is defined by the Crown Prosecution Service as:

The demonstration of unacceptable behaviour by using any means or medium to express views which:

- Encourage, justify or glorify terrorist violence in furtherance of particular beliefs.
- Seek to provoke others to terrorist acts.
- Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
- Foster hatred which might lead to inter-community violence in the UK.

- There is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.
- Pupils may become susceptible to radicalisation through a range of social, personal and environmental factors - it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff are able to recognise those vulnerabilities.

Indicators of vulnerability include:

- Identity Crisis – the student / pupil is distanced from their cultural / religious heritage and experiences discomfort about their place in society.
- Personal Crisis – the student / pupil may be experiencing family tensions; a sense of isolation; and low self-esteem; they may have dissociated from their existing friendship group and become involved with a new and different group of friends; they may be searching for answers to questions about identity, faith and belonging.
- Personal Circumstances – migration; local community tensions; and events affecting the student / pupil's country or region of origin may contribute to a sense of grievance that is triggered by personal experience of racism or discrimination or aspects of Government policy.
- Unmet Aspirations – the student / pupil may have perceptions of injustice; a feeling of failure; rejection of civic life.
- Experiences of Criminality – which may include involvement with criminal groups, imprisonment, and poor resettlement / reintegration.
- Special Educational Need – students / pupils may experience difficulties with social interaction, empathy with others, understanding the consequences of their actions and awareness of the motivations of others.
- However, this list is not exhaustive, nor does it mean that all young people experiencing the above are at risk of radicalisation for the purposes of violent extremism.

More critical risk factors could include:

- Being in contact with extremist recruiters.
- Accessing violent extremist websites, especially those with a social networking element.
- Possessing or accessing violent extremist literature.
- Using extremist narratives and a global ideology to explain personal disadvantage.
- Justifying the use of violence to solve societal issues.
- Joining or seeking to join extremist organisations.
- Significant changes to appearance and / or behaviour.
- Experiencing a high level of social isolation resulting in issues of identity crisis and / or personal crisis.

Preventing Violent Extremism

- Roles and Responsibilities of the Single Point of Contact (SPOC), The SPOC for
- Bishop Stopford's School is Tammy Day (Deputy Head Teacher), who is responsible for:

- Ensuring that staff of the school are aware that you are the SPOC in relation to protecting students/pupils from radicalisation and involvement in terrorism.

- Maintaining and applying a good understanding of the relevant guidance in relation to preventing students/pupils from becoming involved in terrorism, and protecting them from radicalisation by those who support terrorism or forms of extremism which lead to terrorism.

- Raising awareness about the role and responsibilities of Bishop Stopford's School in relation to protecting students/pupils from radicalisation and involvement in terrorism.

- Monitoring the effect in practice of the school's RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.

- Raising awareness within the school about the safeguarding processes relating to protecting students/pupils from radicalisation and involvement in terrorism.

- Acting as the first point of contact within the school for case discussions relating to students / pupils who may be at risk of radicalisation or involved in terrorism.

- Collating relevant information from in relation to referrals of vulnerable students / pupils into the Channel* process.

- Attending Channel* meetings as necessary and carrying out any actions as agreed.

- Reporting progress on actions to the Channel* Co-ordinator.

- Sharing any relevant additional information in a timely manner.

  Channel is a multi-agency approach to provide support to individuals who are at risk of being drawn into terrorist related activity. It is led by the Metropolitan Police Counter-Terrorism Unit, and it aims to
- Establish an effective multi-agency referral and intervention process to identify
- vulnerable individuals;
- Safeguard individuals who might be vulnerable to being radicalised, so that they are not at

risk of being drawn into terrorist-related activity; and
- Provide early intervention to protect and divert people away from the risks they face and reduce vulnerability.

Prevention of Radicalisation through the internet

- Extremists may use the internet, including social media, to share their messages.
- Efforts will be made through our e-safety filtering systems to block inappropriate content.
- Where staff, pupils or visitors find unblocked extremist or terrorist related content, they must report it immediately to the class teacher, Network Manager and Safeguarding lead (Jonathan Seabrook).
- Staff are also aware that children and young people have access to unfiltered internet when using their mobile phones outside of school hours and should be vigilant to comments made about inappropriate content pupils may have viewed at these times.
- The e-safety and internet user policy refers to preventing radicalisation and related extremist content.
- Pupils will be regularly reminded through e-safety lessons and assembly presentations on how to report internet content that is inappropriate or of concern.

Appendix 1 - Acceptable Use Policy

Staff Agreement Form

If malicious or threatening comments are posted on an Internet site about a student or a member of staff, or any content containing extremist views indicating radicalisation :

- Secure and preserve any evidence.
- Inform one of the Child Protection Officers (CPO's)
- Inform and request that comments be removed if the site is administered externally.
- The CPO will send all the evidence to Child Exploitation and Online Protection (**CEOP**) Centre at ww.ceop.gov.uk/contact_us.html
- The CPO will assist in tracing the origin and will inform the Safer Schools Officer as appropriate.

If you are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child.

- Report to, and discuss with one of the named CPO's in school. The CPO will contact parents.
- In consultation with the CPO advise the child on how to terminate the communication and save all evidence.
- The CPO will contact CEOP http://www.ceop.gov.uk/ and consider the involvement of police and social services.
- The CPO will inform the LA (Local Authority) Child Protection Officer.
- The CPO will consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to one of the Child Protection Officers.

Pupils should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

As outlined in the code of conduct policy, we acknowledge that it is important for employees to understand that their own behaviour and the manner in which they conduct themselves with their colleagues, pupils, parents and other stakeholders sets an example and affects the school environment.

The use of the school communications systems and equipment, including electronic e-mail and Internet/Intranet systems, along with their associated hardware and software, are for official and authorised purposes only. However, we realise that the school communication systems may need to be used for other purposes in relation to our roles and therefore we need to be aware of and commit to the following guidelines:

I will only use the school's Email / Internet / Intranet for purposes in a way that it will not interfere with the performance of my professional duties and will be of reasonable duration and frequency as deemed 'reasonable' by the Headteacher and Governing Body.

In using the school's email/internet/intranet for professional purposes I will always use appropriate written language and not discriminate against, harass or victimise anyone I come into contact with, on any grounds, including: race, ethnic or national origin, gender, sexual orientation, marital status, religious or other beliefs, disability, HIV status, age, trade union involvement, having responsibilities for dependants, working on a temporary or part time basis (note that discrimination, harassment and victimisation include the use of language, making remarks, telling jokes, displaying materials or behaving in a way that may be interpreted as discriminatory, even if not directed at a particular individual(s)

I will only use the approved, secure email system(s) for legitimate school interest such as enhancing professional interests or education.

I will not overburden the system or create any additional expense to the school.

I will conduct myself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogative of others. The transmitting or downloading of materials that are obscene, pornographic, threatening, racially or sexually harassing or in any way contravene the Equal Opportunities Policy is prohibited. I understand that Chat Rooms may not be visited nor any sites known to contain offensive material.

I will not keep a personal diary or blog on the Internet (whether at school or at home) where reference is made to the school without authorisation. This is not advisable as such usage could cause harm to the reputation of the school and may undermine the confidence of our parent/carers.

I will report any accidental access to inappropriate materials to the appropriate line manager.

I will not download any software or resources from the Internet that can compromise the network, or is not adequately licensed.

I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.

I will not download or install any software or resources from the Internet on to my PC or laptop without checking with the Network Manager first as to its suitability or compatibility with Enfield County's setup, or is not adequately licensed.

I will only use the designated school camera for recording school events and visits.

I will not transfer images from school visits or events of pupils or colleagues to another system without permission from the schools visit coordinator.

I will not take images of pupils with a personal digital camera without written permission from the Headteacher.

I will not take images of pupils with a personal camera phone.

I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.

I will not allow unauthorised individuals to access my Email / Internet / Intranet.

I understand that all Internet usage will be logged and this information could be made available to my manager on request.

I will only use LA systems in accordance with any corporate policies.

I understand that this policy is binding to all school staff and that it applies to those staff deployed within the school who are employed by external Agencies or the Council and I will adhere to its principles. I understand that Breaches of the Policy and standards expressed in it could result in disciplinary action, including dismissal for serious offences.

I agree to the terms outlined in the AUP:

Name:
(CAPS)

Signature:

Date: