'To unite all things in Christ'. Ephesians 1:10

Bishop Thomas Grant School

Online Safety Policy including IT use and BYOD

'In accordance with the Equality Act, we will strive to eliminate all forms of discrimination, harassment or bullying. All individuals will be treated fairly and will not be treated less favourably on the basis of protected characteristics detailed in the Equality Act including race, gender, age, sexuality, religion and disability'

Review Cycle

Reviewed:	**Approved by:**	**Next Review:**	**Staff Responsible:**
September 2023	Ethos Committee	April 2024	Mr A McCarthy
April 2024	Ethos Committee	September 2024	Mrs A O'Donovan / Mr A McCarthy
October 2024	Ethos Committee	October 2025	Mrs A O'Donovan / Mr A McCarthy
October 2025	Ethos Committee	October 2026	Mrs A O'Donovan / Mr A McCarthy
October 2026	Ethos Committee	October 2027	Mrs A O'Donovan / Mr A McCarthy

'To unite all things in Christ'. Ephesians 1:10

Bishop Thomas Grant School will play a key role in the formation of our young people so that they become responsible Christian adults. Inspired by the message of Jesus Christ they will contribute effectively to society by promoting justice, honesty and charity in all aspects of their lives.

A Voluntary Aided School in the Trusteeship of the Archdiocese of Southwark

The Governing Board of Bishop Thomas Grant School is committed to safeguarding and promoting the welfare of children and young people and expect all staff, volunteers and external agencies to share this commitment.

Contents

Key people / dates 4
Aim 4
Purpose 5
Key Risk Areas 5
Scope 6
Roles and Responsibilities 6
Artificial intelligence (AI) 14
Handling Incidents 16
Actions where there are concerns about a child 16
Handling a sexting incident 18
Education & Curriculum 19
Staff and Governor Training 19
Expected Conduct and Incident Management 19
Incident Management 20
Managing the ICT Systems 20
Network Management 21
Social Networking 23
Data Security 23
EQUIPMENT AND DIGITAL CONTENT 24
Network / internet access on school devices 25
Searching and confiscation 25
Technical Infrastructure and Internet Filtering 26
Dealing with unsuitable and inappropriate activities 26
Reporting Incidents of Misuse 28
Cyber Security / Disaster Recovery Procedures 30
Bring your own Device (BYOD) Sixth Form Students 31
Reviewing and Monitoring Online Safety 32
Communication of this policy 32

Key people / dates

Bishop Thomas Grant School	Designated Safeguarding Lead (DSL) team	Mrs A O'Donovan
	Online-safety lead (if different)	Mr A McCarthy
	Link governor for safeguarding (includes online safety)	Ms M O'Donohue (Safeguarding) Mr S Fernandes
	PSHE/RSHE/RSE lead	Mr D O'Donovan
	Computing Lead	Ms M Edward
	Network manager / other technical support	Mr M Hutchins

Aim

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Bishop Thomas Grant School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of filtering and monitoring through effective collaboration and communication with technical colleagues
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Safeguarding and Child Protection Policy, Behaviour Policy or Anti-Bullying Policy)

Purpose

The purpose of this Policy is to:

- Set out the key principles expected of all members of the school community at Bishop Thomas Grant Secondary School with respect to the use of ICT 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 ICT 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.

Key Risk Areas

Content

Content risk now includes extreme sexual and physical violence extended for AI

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

The following have been introduced as Safeguarding concerns in KCSIE 2025

Conspiracy Theories – These are stories or ideas that claim events are secretly being controlled by powerful groups, often without evidence. They can make children fearful, mistrustful of adults or authorities, and vulnerable to harmful influence. *Example - A child comes across online claims that world leaders are secretly working together in dangerous ways, even though there is no evidence.*

Disinformation – This is false information that is deliberately created and spread to cause harm, mislead, or manipulate people. It is intentional. *Example: A fake news story is published online to influence how people vote or to stir up fear about a group of people.*

Misinformation – This is a false or misleading information that is shared by someone who believes it to be true. They are not trying to cause harm, but what they pass on is still wrong and can mislead others. *Example: A parent shares an inaccurate health claim on social media, thinking it would help others.*

Contact

Now includes generative AI applications simulating adults posing as children

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

Conduct

Now includes explicit images generated using AI

- 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)

Commerce

- Online Gambling
- Inappropriate advertising
- Phishing or financial scams

Scope

This policy applies to all members of the Bishop Thomas Grant School community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, governors, volunteers, contractors, students/Students, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and Responsibilities

Roles:

- All Staff
- Headteacher/Principal
- Designated Safeguarding Lead / Online Safety Lead
- Governing Body, led by Online Safety / Safeguarding Link Governor
- PSHE / RSHE Lead/s
- Computing Lead
- Subject / aspect leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Students
- Parents/carers
- External groups including parent associations

All staff

Key responsibilities:

- Read and follow this policy in conjunction with the school's main safeguarding policy and the relevant parts of Keeping Children Safe in Education

- Understand that online safety is a core part of safeguarding and part of everyone's job – never think that someone else will pick it up. Safeguarding is often referred to as a jigsaw puzzle – you may have the missing piece, so do not keep anything to yourself. Record online-safety incidents in the same way as any safeguarding incident; report in accordance with school procedures
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are; notify them not just of concerns but also of trends and general issues you may identify. Also speak to them if the policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon
- Sign and follow the staff Acceptable Use of IT policy and code of conduct/handbook
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for Students)
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (be aware of what appropriate filtering and monitoring systems are in place and how they keep children safe).
- Follow best-practice pedagogy for online-safety education, avoiding scaring, victim-blaming language and other unhelpful prevention methods.
- When supporting Students remotely, be mindful of additional safeguarding considerations – refer to the schools Remote Learning Policy.
- Carefully supervise and guide Students when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online sources and classroom resources before using for accuracy and appropriateness.
- Encourage students to follow their Acceptable Use of IT Policy at home as well as at school, remind them about it and enforce school sanctions.
- Take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter - this includes bullying, sexual violence and harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues
- Model safe, responsible and professional behaviours in your own use of technology. This includes outside school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. Please follow the Staff Code of Conduct or more guidance can be found in this Online Reputation guidance for schools.

Headteacher – Ms B Boyle

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the designated safeguarding lead team and ensure they work with technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles
- Liaise with technical colleagues on a regular basis to have an understanding and awareness of filtering and monitoring provisions and manage them effectively – in particular understand what is blocked or allowed for whom, when, and how. Note that KCSIE strengthens the wording for this.
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Support safeguarding leads and technical staff as they review protections for Students in the home and remote-learning procedures, rules and safeguards.
- Assign responsibility to a nominated member of staff to carry out online searches with consistent guidelines as part of due diligence for the recruitment shortlist process (this new addition has come into KCSIE 2022 for the first time)
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of Students, including risk of children being radicalised
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead / Online Safety Lead – Mrs A O'Donovan / Mr A McCarthy

Key responsibilities

- Work with the HT and technical staff to review protections for Students in the home and remote-learning procedures, rules and safeguards.

- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective whole school approach to online safety that empowers the school to protect and educate the whole school community in their use of technology and establish mechanisms to identify, intervene in and escalate any incident where appropriate."
- Ensure ALL staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated. Liaise with the Headteacher and Chair of Governors to ensure that ALL governors and trustees undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school)
- Work with the Headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance and beyond, in wider school life.
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents.
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for Students to disclose issues when off site.
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are also aware. Liaise with technical teams and ensure they are implementing not taking the strategic decisions on what is allowed and blocked and why.

- Ensure KCSIE 'Part 5: Sexual Violence & Sexual Harassment' is understood and followed throughout the school and that staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and is not dismissed as banter (including bullying).
- Facilitate training and advice for all staff, including supply teachers:
- all staff must read KCSIE Part 1 and all those working with children
- cascade knowledge of risks and opportunities throughout the organisation

Governing Body, led by Online Safety / Safeguarding Link Governor – Mrs M O'Donohue and Mr S Fernandes

Key responsibilities (quotes are taken from Keeping Children Safe in Education)

- Approve this policy and strategy and subsequently review its effectiveness,
- Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Ensure appropriate filters and appropriate monitoring systems are in place
- Ask about how the school has reviewed protections for Students in the home (including when with online tutors) and remote-learning procedures, rules and safeguards
- Ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety) with the appropriate status and authority, time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and Headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated in line with advice from the local safeguarding partners integrated, aligned and considered as part of the overarching safeguarding approach."
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school approach to online safety with a clear policy on the use of mobile technology."

PSHE / RSHE Lead/s – Mr D O'Donovan

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their students' lives
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help Students to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where Students need extra support or intervention through tests, written assignments or self-evaluations, to capture progress"
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Computing Lead – Ms M Edward

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with Acceptable Use Agreements

Subject / aspect leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the new RSHE curriculum, and model positive attitudes and approaches to staff and Students alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element

Network Manager/technician – Mr M Hutchins

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology. Note that KCSIE changes expect a great understanding of technology and its role in safeguarding, so help DSLs and SLT to understand systems, settings and implications.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE.
- 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
- Work closely with the designated safeguarding lead / online safety lead / data protection officer/ RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems and filtering, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Monitor the use of school technology, and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Headteacher to ensure the school website meets statutory DfE requirements

Data Protection Officer (DPO) –Liaison with Judicium

Key responsibilities:

- Be aware of references to the relationship between Data Protection and Safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
  "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent (DPA, Part 2, 18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children."

- The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until Student is aged 25 or older)'. However, some local authorities require record retention until 25 for all Student records.
- Work with the DSL, Headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors (including tutor)

Key responsibilities:

- Read, understand, sign and adhere to an Acceptable Use Policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a Student. The same applies to any private/direct communication with a Student.

Students

Key responsibilities:

- Read, understand, sign and adhere to the student/Student Acceptable Use of IT policy and review this annually
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.
- Treat home learning during any isolation/quarantine or bubble/school lockdown in the same way as regular learning in school and behave as if a teacher or parent were watching the screen.

Parents/carers

Key responsibilities:

- Read, Sign and promote the schools 'School ICT Facilities Permission Form' (Appendix 1) and encourage their children to follow this.
- Talk to the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, Students or other parents/carers.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available in the Online Tutors – Guidance for Parents and Carers poster at parentsafe.lgfl.net, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online
- Encourage children to engage fully in home-learning, whether for homework or during any school closures or isolation and flag any concerns
- Support the child during any home learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.

External groups including parent associations – School PTA

Key responsibilities:

- Any external individual/organisation will sign an IT Acceptable Use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, Students or other parents/carers

Artificial intelligence (AI)

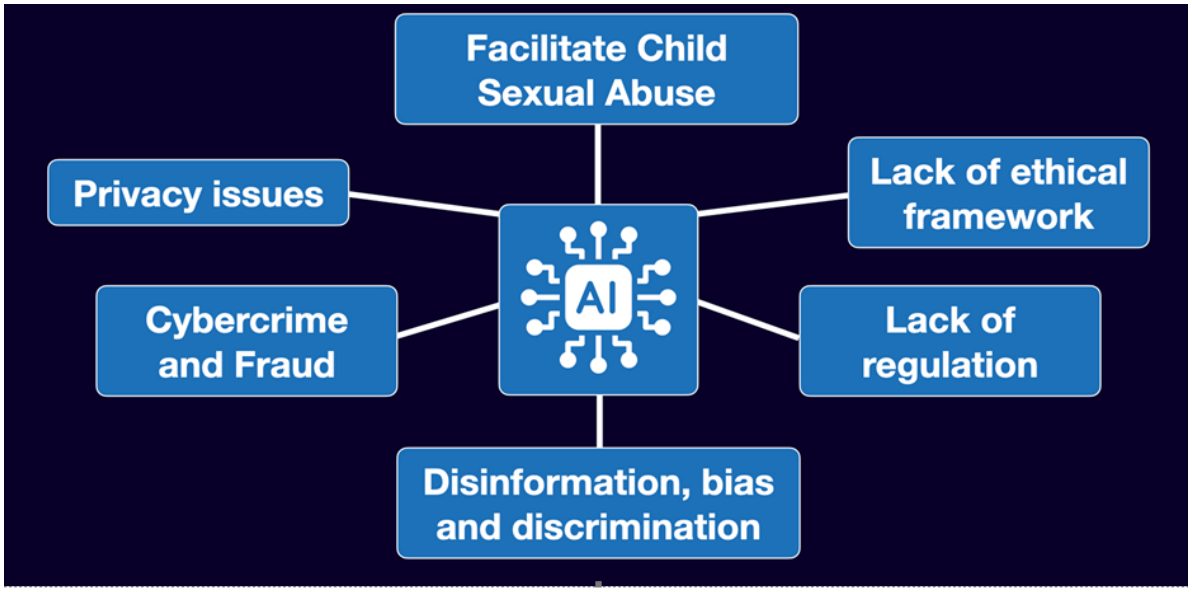
We have an AI policy following current guidance however this is constantly under review as this an area that changing rapidly. All staff must always consider the ethics and promote these with students following the guidance that was issued at the start of term. Staff are aware of AI and are being trained in how to recognise signs of AI abuse.

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: learner support, teacher support, and school operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of learners and staff remains central to our approach.

KCSIE 2026 recognises that learners may be subject to harmful online interaction with other users or generative AI applications that simulate these.

Some potential harms:



The school will:

- Check age limits and terms of service
- Choose enterprise-grade tools with organisational control
- Create interim guidance for staff and students
  - Update key policies and complete a Data Protection Impact Assessment (DPIA)
  - Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Comply with relevant law and guidance, including Keeping Children Safe in Education (KCSIE) and UK GDPR.
- Provide training and guidance for staff and governors on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping learners understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.
- All AI generated concerns are considered safeguarding issues and must be referred to DSL

The Online Safety Bill is now law, and the following are now crimes:

- Cyberflashing – illegal to send unsolicited sexual images intended to alarm or distress
- Epilepsy trolling – criminal to send flashing images aiming to trigger seizures or cause distress
- Threatening communications – Sending threats of serious harm, death, or violence is a standalone

offence

- Encouraging serious self-harm – Offence to promote or encourage serious self-harm online, even if harm doesn't occur
- Sharing intimate images (including deepfakes) – offence to share or threaten to share sexual images without consent, including AI-generated content.

All aspects will now be incorporated into school ICT and PSHE lessons, including students being made aware of what age verification means.

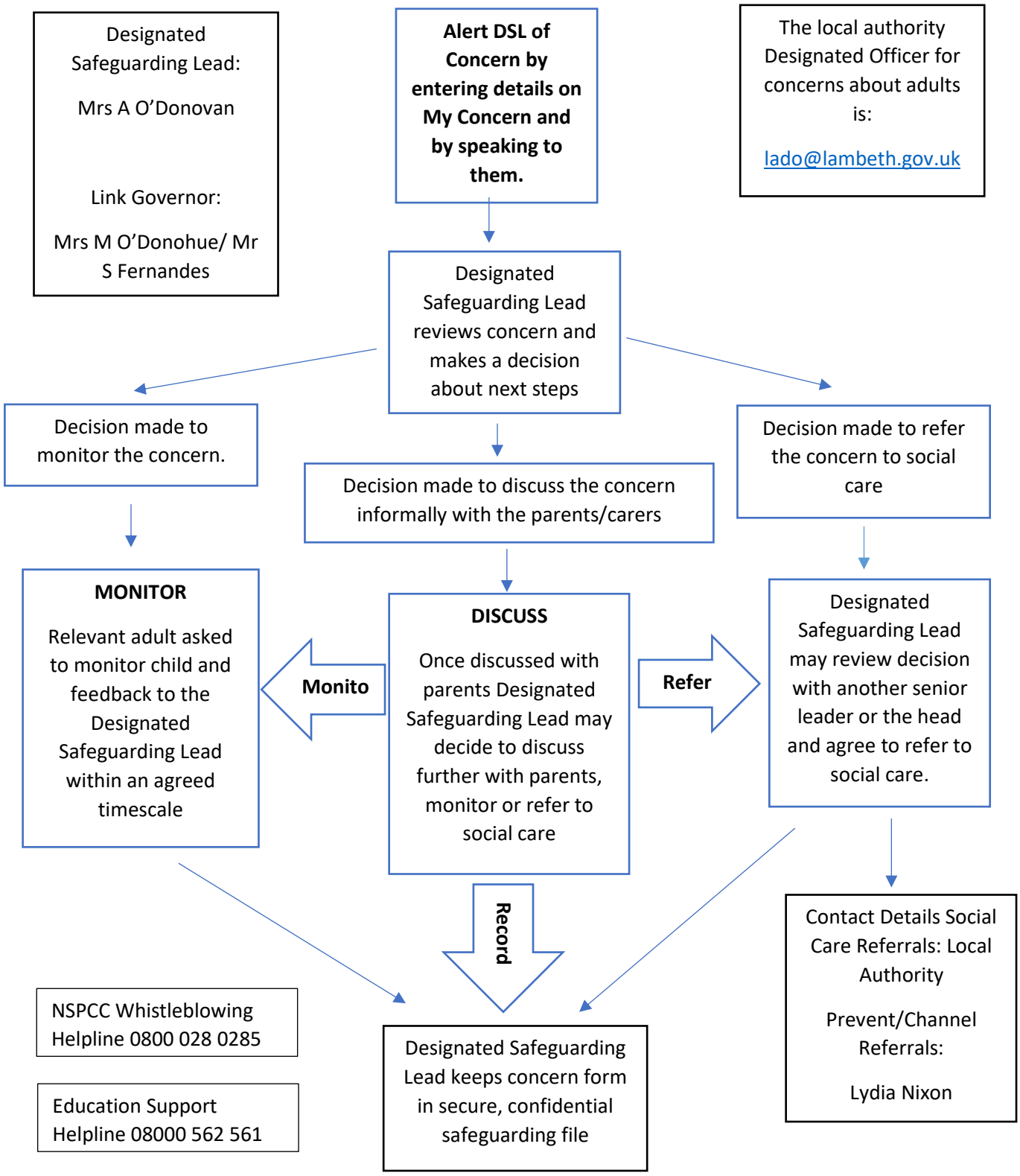
From 25 July 2025, all pornographic website accessible in the UK must have effective age verification systems in place (such as ID checks or facial age estimation). Age verification also in places for other harmful content, for example eating disorders or self-harm.

Handling Incidents

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

Actions where there are concerns about a child

The following flow chart is taken from the child protection policy document. As outlined previously, online safety concerns are no different to any other safeguarding concern. Same procedure applies for online safety incidents


Designated Safeguarding Lead:
Mrs A O'Donovan
Link Governor:
Mrs M O'Donohue/ Mr S Fernandes
Alert DSL of Concern by entering details on My Concern and by speaking to them.
The local authority Designated Officer for concerns about adults is:
lado@lambeth.gov.uk
Designated Safeguarding Lead reviews concern and makes a decision about next steps
Decision made to monitor the concern.
Decision made to discuss the concern informally with the parents/carers
Decision made to refer the concern to social care
MONITOR
Relevant adult asked to monitor child and feedback to the Designated Safeguarding Lead within an agreed timescale
Monito
DISCUSS
Once discussed with parents Designated Safeguarding Lead may decide to discuss further with parents, monitor or refer to social care
Refer
Designated Safeguarding Lead may review decision with another senior leader or the head and agree to refer to social care.
Record
NSPCC Whistleblowing Helpline 0800 028 0285
Education Support Helpline 08000 562 561
Designated Safeguarding Lead keeps concern form in secure, confidential safeguarding file
Contact Details Social Care Referrals: Local Authority
Prevent/Channel Referrals:
Lydia Nixon

Handling a sexting incident

There should always be an initial review meeting, led by the Designated Safeguarding Lead. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people

When assessing the risks the following should be considered:

  - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the student in the imagery?
  - Are there any adults involved in the sharing of imagery?
  - What is the impact on the students involved?
  - Do the students involved have additional vulnerabilities?
  - Does the young person understand consent?
  - Has the young person taken part in this kind of activity before?

- If a referral should be made to the police and/or children's social care
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the students involved – in most cases parents should be involved

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further Information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the Designated Safeguarding Lead is confident that they have enough information to assess the risks to students involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

Education & Curriculum

Bishop Thomas Grant School:

- has a clear, progressive online safety education programme as part of the Computing curriculum, PSHE 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 student 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 students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure students only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and Governor Training

Bishop Thomas Grant School:

- regular training for staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with training, information and guidance on the IT Acceptable Use Policy and the school's Acceptable Use Agreements.

Expected Conduct and Incident Management

At Bishop Thomas Grant School **all users**:

- are responsible for using the school ICT systems in accordance with the relevant IT 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;

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

Parents/Carers

- should provide consent for students 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

At Bishop Thomas Grant 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, IWF) 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 students 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 the ICT Systems

Bishop Thomas Grant School:

- informs all users that Internet/email/computer use is monitored;
- has the educational filtered secure broadband connectivity;
- uses a 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 user-level filtering where relevant, e.g. YouTube access;
- ensures network health through use of Sophos anti-virus software or equivalent;
- uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure
- file/email to send 'protect-level' (sensitive personal) data 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 all 3rd party support to ensure any concerns about the system are

communicated so that systems remain robust and protect students.

- Will ensure that all school IT equipment and software will be updated regularly with appropriate virus protection and appropriate filtering. This will be managed remotely by the School IT Network Manager.

Network Management

Bishop Thomas Grant School

- Uses individual, audited log-ins for all users;
- Uses expiring 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 any relevant services and policies/requires any Technical Support Provider to be up-to-date with any relevant services and policies;
- Has daily back-up of school data;
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the school will conform to UK data protection requirements; Storage of data online, will conform to the GDPR data protection regulations where storage is hosted within the EU.

To ensure the network is used safely, the 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 the service is through a unique, audited username and password. The same credentials are used to access the school's network. We also use the same username and password for access to our school's network;
- All students 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 students should never be allowed to log-on or use teacher and staff logins. This is outlined in the Acceptable Use of IT Policy.
- Has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- 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.
- 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;
- The school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;

- Ensures that all student 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), DfE S2S or Egress;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- The school makes it clear that staff and students 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 regularly at least 3 times a year
- We require staff using critical systems to use two factor authentication.

E-mail

The school:

- Provides staff with an email account for their professional use Microsoft Office 365 and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or students 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 security technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Students

- We use Microsoft Office 365 as a student email system which is intentionally 'anonymised' for student protection.
- Students in lower year groups are only allowed to send/receive email to/from authorised senders or domains.
- Students are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff

- Staff will use LA or school provided e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff are careful with highly sensitive emails to transfer staff or student personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Headteacher, 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 website 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 students' names when saving images in the file names or in the tags when publishing to the school website

Social Networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- 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 students, but to use the school's preferred system for such communications.

School staff will ensure that in private use

- No reference should be made in social media to students, parents/carers or school staff
- School staff should not be online friends with any student. Any exceptions must be approved by the Headteacher.
- 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 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.

Students

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our [age appropriate] student IT Acceptable Use Agreement.

Parents

- Parents are reminded about social networking risks and protocols through our parental IT Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

Data Security

Strategic and operational practices

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- Files are also stored on Microsoft Office 365 (SharePoint & OneDrive), different levels of access are given depending on role.
- We require staff to log-out of systems when leaving their computer, but also enforce lock- out after 5 minutes idle time.

- We use the RMUnify and Microsoft Office 365 or other similar identity management platform that connects with our Management Information System, for creation of online user accounts for access to the School systems and emails.
- We use RMUnify which integrates our MIS with Microsoft Office 365.
- All servers are in lockable locations with limited access to only designated 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 or approved data destruction companies.

EQUIPMENT AND DIGITAL CONTENT

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device[1]	Student owned (6th Form and SEN	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	No	No	No	No
Internet only	No	No	Yes	Yes	Yes	Yes
No network access	No	No	No	No	No	No

- **Students** enrolled into the Schools Sixth Form are allowed to bring mobile phones. They may use mobile phones during lunch break at designated areas, but not when moving around the school buildings.
- During lessons, phones must remain turned off at all times, unless the teacher has given express permission as part of the lesson. But students will not be allowed to take any photos or videos during this time.

  Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to sanctions dependent on the situation and the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to Students in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section in

this policy and Data protection and data security section of this policy. Child/staff data should never be downloaded onto a private phone.

- Staff are allowed to use personal mobile devices in school. The access to Network resources including Internet is down to the discretion of IT Support and the SLT.
- Personal devices to both staff and student **will not** be covered by insurance or entitled to technical support.
- Filtering of the internet connection to these devices will be at a high level.
- Filtering and monitoring process will be reviewed annually
- School data is not to be taken home on devices without prior consent and encryption.
- The School will have the right to inspect any mobile device which is suspected to been used inappropriately. Staff/Student agree to hand over any required login information when requested. Failure to do this could lead to disciplinary actions. Please see linked policies.

- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.

Network / internet access on school devices

- **Students** are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet for school-related internet use / limited personal use within the framework of the Acceptable Use of IT Policy. All such use is monitored. Access to personal files or networked files can only be accessed though School onsite devices or using the school remote access system.

- **Volunteers, contractors, governors** can access the guest wireless network but have no access to networked files/drives, subject to the Acceptable Use of IT Policy. All internet traffic is monitored.

- **Parents** have no access to the school network or wireless internet on personal devices.

- **Trips / events away from school**
  For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher/Principal and staff authorised by them have a statutory power to search students property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Full details of the school's search procedures are available in the school Behaviour Policy https://www.btg.ac/About-BTG/Policies

Technical Infrastructure and Internet Filtering

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.

The school filtering and monitoring processes are reviewed annually.

- **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 IT Support who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The IT Co-ordinator and Network manager are 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
- 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. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.

Dealing with unsuitable and inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying is banned and will lead to Police intervention and possible criminal prosecution. There maybe activities that may, generally, be legal but would be inappropriate in our school context, either because of the age of the users or the nature of those activities such as inappropriate searching e.g. for gaming and song lyrics.

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:

Please also refer to the Safeguarding Policy.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material,	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	X
	Promotion of any kind of discrimination/Hate Crime				X	X
	threatening behaviour, including promotion of physical violence or mental harm				X	X
	Promotion of extremism or terrorism				X	X
	Sexual Harassment Online					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	X
Using school systems to run a private business					X	X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	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	
On-line gaming (educational)					
On-line gaming (non-educational)					X
On-line gambling					X
On-line shopping / commerce					
File sharing					X
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting e.g. Youtube				X	

Reporting Incidents of Misuse

Incidents should be reported to a member of the safeguarding team and the Network Manager should be instructed to carry out necessary precautions. 'Smoothwall Monitor' is likely to report many of the incidents above and these will be dealt with and investigated by the School Safeguarding Team and possible referrals to Social Service Police or LADO

Incidents

It is expected that all members of the school community will be responsible users of digital technologies, who understand and follow the school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion or a report, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the

content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority Group or national / local organisation (as relevant).
    - Police involvement and/or action
    - Contacting parents
    - If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - Incidents of 'grooming' behaviour
    - The sending of obscene materials to a child
    - Adult material which potentially breaches the Obscene Publications Act
    - Criminally racist material
    - Promotion of terrorism or extremism
    - Other criminal conduct, activity or materials
    - Sexual Harassment
    - Hate Crime
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

'Smoothwall Monitor' will record misuse detected and take a screenshot of the incident with the user credentials identified, the device where the incident occurred with the date and time of the incident.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures the school has in place.

Digital images and video

When a student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long.

Parental consent is generally recorded via the Sims Parent App.

The use of consent will be used for the following;

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication

- For social media

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any Students shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of Students, and where these are stored. At Bishop Thomas Grant School, we would like no member of staff to use their personal phone to capture photos or videos of Students, however some circumstances will allow this with permission from the Headteacher.

Photos are stored on the school systems in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

As part of our PSHE young people think about their online reputation and digital footprint, aim to be a good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Students 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

Students are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Students 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 / or a friend are subject to bullying or abuse.

Cyber Security / Disaster Recovery Procedures

A disaster can be caused by many events resulting in BTG's IT department not being able to perform some or all of their regular roles and responsibilities for a period of time. Bishop Thomas Grant IT Support defines disasters as the following:

- *One or more vital systems are non-functional*
- *All systems are non-functional*
- *The building and all systems are non-functional*

The following events can result in a disaster requiring school action;

- *Environmental disaster (flooding, hurricane, fire, etc.)*
- *Hardware failure / server room issue*

- *Power outage*
- *Theft*
- *Cyber Attack / Virus outbreak*
- *Deliberate attack*
- *Terrorist attack*
- *Human error*

The top priority of the IT Department will be to bring all of the organisation's IT environments back to business-as-usual as quickly as possible. This includes:

- *Preventing the loss of the organisation's resources such as hardware, data and physical IT assets*
- *Minimizing downtime related to IT*
- *Keeping the school running in the event of a disaster*

Cyber Security Incident Procedure

If required (In the event of a Virus or Cyber-attack) the Schools Network will be taken offline to prevent further spread/damage to the system.

With the system being offline, BTG IT Support with the support of 3rd Party suppliers will check each system individually for any damage / Affected data and will notify all affected persons'/Parties'.

The affected systems will recovered using an up to date unaffected backup of the network.

Systems which have not been compromised will be powered on back to normal state after inspection.

The aim would be to have as many systems bought back online as quickly as possible to ensure teaching can resume, whilst further repairs/Inspections are carried out.

Bring your own Device (BYOD) Sixth Form Students

Students who attend the Sixth Form at the school will be allowed to bring in personal devices to be used to aid their education. Exceptions to this may apply to any students in other year groups for learning or medical needs. The Bishop Thomas Grant Safeguarding Team will be required to give permission for this.

All devices will subject to the following conditions;

- The laptop will be the sole responsibility of the student. Any theft/damage to the device is not the responsibility of the school to replace or repair
- When using the device in school, the device must be connected to the BTG WIFI. Any other connections to the internet e.g. Personal hotspots are not permitted. Any students found to be using other methods of connection will be sanctioned.
- The student agrees the device is only to be used to aid in their education, Any misuse to the device could lead to them not being able to use their own device in school and possibly further sanctions
- For students in years 7 -11 who have been given permission to bring their own device due to learning or medical needs, will agree to have the school monitoring software (smoothwall)

installed onto the device before this can be used in school

CENMAC Devices

For some users a device from CENMAC might be supplied to aid in their education.

All devices supplied by CENMAC will;

- Be kept at school
- Have Smoothwall Monitoring software installed
- Parent/Carers sign the IT Acceptable use agreement
- Will be used in all terms set within this policy

Reviewing and Monitoring Online Safety

This policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE policy).

- This policy will be reviewed every 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 this policy will be disseminated to all members of staff and students.

Communication of this policy

The policy will be communicated to staff, students and the wider community in the following ways:

- Policy to be posted on the school's website
- 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 students at the start of each year.
- Acceptable Use agreements to be issued to whole school community, on entry to the school.

Appendix 1

SCHOOL ICT FACILITIES PERMISSION FORM

Student name(s): _____

Please read the Acceptable Use of IT at Bishop Thomas Grant School booklet, which has been sent t you via email, in addition to this form then complete this form accordingly.

As the parent or legal guardian of the above student, I grant permission for my daughter or son to have access to use the Internet, and other ICT facilities at school.

I know that my daughter or son will have to electronically accept/sign an Online Safety Agreement Form.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials. These steps include using internet filtering services, software that monitors all computer usage and records any misuse, evidence of which will be used to support the schools behaviour management system, restricted access e-mail, and teaching online safety skills to students.

I understand that the school can check my child's school computer files, and the Internet sites they visit, in and out of school and that if parents or students have concerns about online safety or online behaviour that they will contact the school.

I understand the School will issue my child with an email address and that a Senior Member of staff or Technical Team can access the content if the School feels it is necessary. I understand that no other email should be used by my child to communicate with School staff. I understand that my child should not abuse the School email system in any way. I understand my child should not use any form of Social Media to contact School staff and I will report this to the School if I feel this is happening.

I understand that Bullying, in any form, is seen as a severe breach of school rules and Online Bullying is no different. Any attempt to bully any member of the school community either inside or outside the school by use of the internet and all electronic formats including phones and all social media may lead to permanent exclusion from Bishop Thomas Grant School, legal action being taken and Metropolitan Police involvement.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent/Carer Name: _____

Parent/Carer Signature: _____ Date: _____

The school is registered under the Data Protection Act 2018 for holding personal data. We take the protection of your data very seriously. If you would like to know more about how we use, store and dispose of your data, please refer to the privacy notices and the data protection policy on our website.