Brunel College, Online Safety Policy - 2023/4

Introduction

Key people / dates

Brunel College	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Kerry Williams
	Deputy Designated Safeguarding Leads / DSL Team Members	Wendy Moscrop
	Link Trustee for safeguarding	Morven Fletcher
	Curriculum leads with relevance to online safeguarding and their role	Ali Marshall Cirriculum Lead/ PSHE Kerry Williams PSHE
	Network manager / other technical support	John Heagren Wiltshire Technology. Guy Griffith.
	Date this policy was reviewed and by whom	February 2024 SLT and Trustees
	Date of next review and by whom	April 2025 DSL/ Headteacher.

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into your school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy should be a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, pupils and parents in writing and reviewing the policy and make sure the policy makes sense and it is possible to follow it in all respects. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Pupils could help to design a version in language their peers

understand or help you to audit compliance. Acceptable Use Agreements (see appendices) for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

Who is in charge of online safety?

KCSIE makes clear that "the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety)." The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for PSHE will plan the curriculum for their area, it is important that this ties into a whole-school approach.

What are the main online safety risks in 2023/2024?

Current Online Safeguarding Trends

In our school over the past year, we have particularly noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our students:

- Using proxy server to access filtered webpages and media such as films, when using school iPads.
- Students using threatening language and sharing inappropriate images via social media, when using their own devices that connect to the Internet, via their own ISP, when in school.
- Filming of fights on personal devices and sharing these videos.

Nationally, some of the latest trends of the past twelve months are outlined below. These should be reflected in this policy and the acceptable use agreements we use, and seen in the context of the 5 Cs (see KCSIE for more details), a whole-school contextual safeguarding approach that incorporates policy and practice for curriculum, safeguarding and technical teams.

We may be updating this policy during the year to reflect any changes resulting from the Online Safety Bill being passed into law.

Self-generative artificial intelligence has been a significant change, with students having often unfettered access to tools that generate text and images at home or in school. These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for information, but also in terms of plagiarism for teachers and above all safety: none of the mainstream tools have end-user safety settings, most have an age limit of 13 or even 18 and in spite of basic rude words not delivering results, will easily produce inappropriate material. Schools not only need to tackle this in terms of what comes into school but also educating young people and their parents on use of these tools in the home.

The continued cost-of-living crisis has meant that children have spent more time online and therefore exposed to all manner of online harms as families have had to cut back on leisure activities and the public provision of free activities for young people has reduced further.

Against this background, the Ofcom 'Children and parents: media use and attitudes report 2023' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp,

TikTok and Snapchat increased yet further. As a school we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore remember to remind about best practice while remembering the reality for most of our students is quite different.

This is striking when you consider that over 95 percent of students have their own mobile phone by the end of Year 7, and the vast majority do not have safety controls or limitations to prevent harm of access to inappropriate material. This is particularly pertinent given that 130,556 cases of self-generated child sexual abuse material were found of 11-13 year olds (Internet Watch Foundation Annual Report). These were predominantly (but importantly not only) girls; it is important also to recognise more and more older teenage boys being financially extorted after sharing intimate pictures online.

In the past year, more and more children and young people used apps such as snapchat as their source of news and information, with little attention paid to the veracity of influencers sharing news. The 2023 Revealing-Reality: Anti-social-Media Report highlights that this content is interspersed with highly regular exposure to disturbing, graphic and illegal content such as fights, attacks, sexual acts and weapons. At the same time, the Children's Commissioner revealed the ever younger children are regularly consuming pornography and living out inappropriate behaviour and relationships due to 'learning from' pornography. This has coincided with the rise of misogynistic influencers such as Andrew Tate, which had a significant influence on many young boys over the past year which schools have had to counter.

From the many schools that LGfL spoke to over the past year, there was a marked increase in the number of schools having issues with fights being filmed and shared, a disturbing increase in the cases of self-harm and sexual abuse being coerced with threats of violence (many even in primary schools).

There has been a significant increase in the number of fake profiles causing issues in schools, both for schools – where the school logo and/or name have been used to share inappropriate content about students and also spread defamatory allegations about staff, and also for students, including where these are used to bully others (sometimes even pretending to be one student to bully a second student).

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff
- Clearly reflected in the Acceptable Use Agreements (AUAs) for students and staff

Brunel College, Online Safety Policy - 2023/4

Contents

Introduction 1

Key people / dates 1

What is this policy? 1

Who is it for; when is it reviewed? 1

Who is in charge of online safety? 2

What are the main online safety risks in 2023/2024? 2

How will this policy be communicated? 3

Contents 4

Overview 6

Aims 6

Further Help and Support 6

Scope 7

Roles and responsibilities 7

Education and curriculum 7

Handling safeguarding concerns and incidents 8

Actions where there are concerns about a child 9

Sexting – sharing nudes and semi-nudes 11

Upskirting 12

Bullying 12

Child-on-child sexual violence and sexual harassment 12

Misuse of school technology (devices, systems, networks or platforms) 12

Social media incidents 13

Data protection and cybersecurity 14

Appropriate filtering and monitoring 14

Messaging/commenting systems (incl. email, learning platforms & more) 15

Authorised systems 15

Behaviour / usage principles 16

Online storage or learning platforms 17

School website 17

Digital images and video 17

Brunel College, Online Safety Policy - 2023/4

Social media 18

Our SM presence 18

Staff, pupils' and parents' SM presence 19

Device usage 20

Personal devices including wearable technology and bring your own device (BYOD) 21

Use of school devices 21

Searching and confiscation 22

Appendix – Roles 23

All staff 23

Headteacher/Principal – Craig Noble 23

Designated Safeguarding Lead / Online Safety Lead – Kerry Williams 24

Trustees, led by Online Safety / Safeguarding Link Trustee – Morven Fletcher 26

PSHE Lead – Ali Marshall/ Kerry Williams 27

Subject leaders 27

Network Manager/other technical support roles – John Heagren/Guy Griffith 27

Data Protection Officer (DPO) – Nicki Wright 28

Volunteers and contractors 29

Students 29

Parents/carers 29

Brunel College, Online Safety Policy - 2023/4

Overview

Aims

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

- Setting out expectations for all the Brunel College 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 all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- 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 Behaviour Policy or Anti-Bullying Policy)

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Child Protection & Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the headteacher will handle referrals to Wiltshire DOFA.

London Grid for Learning (a regional school ISP) have extensive resources and have a list of curated links to extremal support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people. **reporting.lgfl.net**

Brunel College, Online Safety Policy - 2023/4

Scope

This policy applies to all members of the Brunel College community (including teaching and support staff, governors, volunteers, contractors, students/pupils, 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

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Depending on their role, all members of the school community should **read the relevant section in Annex A of this document** that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the annex.

In 2023/2024, it is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

Education and curriculum

It is important that schools establish a carefully sequenced curriculum for online safety that builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils – dedicated training around this with curriculum mapping for RSE/PSHE and online safety leads is available at safetraining.lgfl.net

PSHE is the primary subject that has the clearest online safety links, RSE is delivered through PSHE lessons and, school nurse and pastoral support. Students have close links to pastoral leads who provide regular online safety support to students.

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, 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 pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place). "Parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online" (KCSIE 2023).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

Co-Connect are our Internet Service provider and publish a blog on their website with information and resources Co-Connect Blog

Brunel College subscribe to National Online Safety and staff have access to their resources.

At Brunel College, we recognise that online safety and broader digital resilience must be thread throughout the curriculum.

Annual reviews of curriculum plans/ schemes of work (including for SEND pupils) are used as an opportunity to review and embed online safety.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as a curriculum area).

General concerns must be handled in the same way as any other safeguarding concern. All stakeholders should talk to the Designated Safeguarding Lead, who will advise and inform the Headteacher of decision made.

Support staff, particularly Heads of Year, will often have further insight and opportunity to discover issues, when working one to one with students; supporting them with off-site activities and during Thrive and ELSA sessions.

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Sexual Harassment / Child-on-Child Abuse Policy (if separate)

- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Agreements
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cybersecurity policy

This school commits to take all reasonable precautions to ensure safeguarding pupils online, but recognises that incidents will occur both inside and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Trustees and Wiltshire DOFA as appropriate. Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 32-34 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

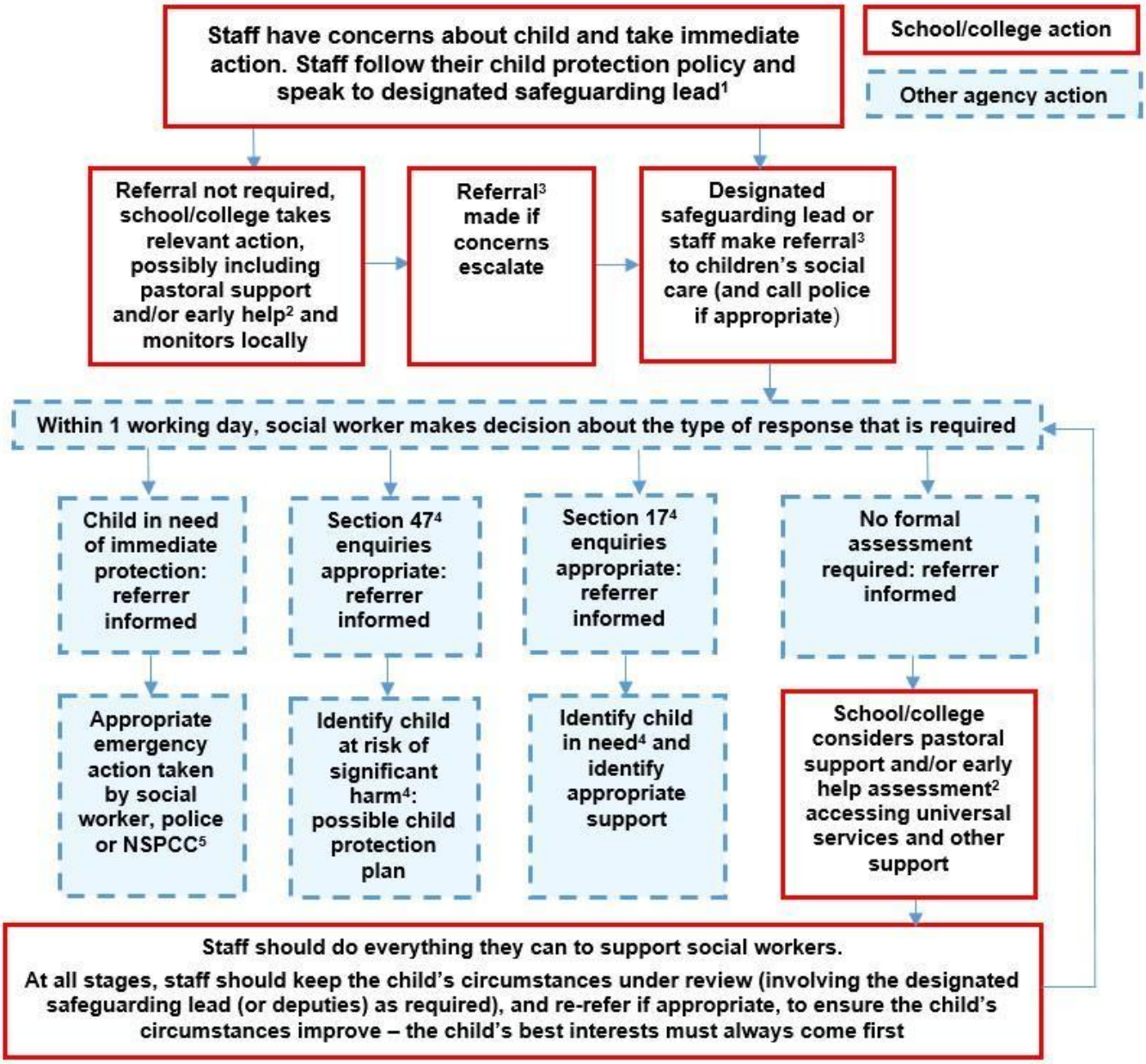
We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider particularly concerning or which breaks the law (particular procedures are in place for sexting and upskirting; see section below).

The school should evaluate whether reporting procedures are adequate for any future closures/ lockdowns/ isolation etc and make alternative provisions in advance where these might be needed.

Actions where there are concerns about a child

The following flow chart (it cannot be edited) is taken from page 22 of Keeping Children Safe in Education 2022 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

Brunel College, Online Safety Policy - 2023/4

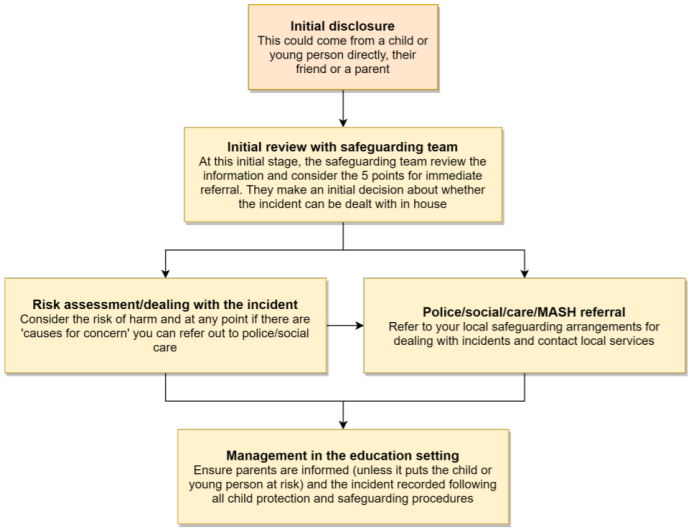


Sexting – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.



***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child on child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

It is important to be aware that in the past 12 months there has been an increase in anecdotal reports of fights being filmed and fake profiles being used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Child-on-child sexual violence and sexual harassment

Part 5 of Keeping Children Safe in Education covers 'Child-on-child sexual violence and sexual harassment' and it would be useful for all staff to be aware of many aspects outlined there to support a whole-school response; case studies are also helpful for training.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour. This behaviour will not be tolerated at Brunel College and the usual safeguarding pathways will be used to manage the use of misogynistic language or behaviour online,

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy which is explained to students and signed by students during their induction, as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

The new responsibilities for filtering and monitoring, led by the DSL and following the new DfE standards, may mean that more of such incidents may be discovered, but the school will do its best to remind pupils and staff of this increased scrutiny regularly.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Brunel College community. These are also governed by school Acceptable Use Policies and the school social media policy.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Brunel College will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policies, and cybersecurity policy which can be found on the school website. It is important to remember that there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cybersecurity for the first time in 2023.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

Keeping Children Safe in Education has long asked schools to ensure "appropriate" webfiltering and monitoring systems which keep children safe online but do not "overblock".

Since KCSIE 2023, in recognition of the importance of these systems to keeping children safe, the Designated Safeguarding Lead now has lead responsibility for filtering and monitoring (see page 1 for the DSL name and the named governor with responsibility for filtering and monitoring).

Schools are also asked to follow the new DfE filtering and monitoring standards, which require them to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

The DSL will work closely with staff who support the running of the school network, Internet access

ALL STAFF need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via email to the DSL regarding students or staff evading filtering systems and to Guy Griffith if an online teaching tool they need is filtered.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUAs and regular training reminders in the light of the annual review and regular checks that will be carried out. The DSL will receive automatic email alerts that will identify staff and students who are accessing potentially concerning websites. Staff and students will be made aware that they will be asked to provide further information and the DSL will manage as appropriate.

Brunel College, Online Safety Policy - 2023/4

It is very important that schools understand the difference between filtering and monitoring, the meaning of overblocking and other terms, as well as how to get the best out of systems. There are guidance videos and flyers to help with this at https://safefiltering.lgfl.net and training is provided for all staff / safeguarding teams / technical teams as appropriate.
At Brunel College

- web filtering is provided by Co-Connect through NetSweeper on school site and a NetSweeper client is installed on student iPads before they can be used at home.
- overall responsibility is held by the DSL with further support from the Headteacher
- technical support and advice, setup and configuration are from John Heagren from Wiltshire Technology.
- regular checks are made each term by Guy Griffith to ensure filtering is still active and functioning everywhere. The date and details of the checks done are recorded in a spreadsheet and held with the DSL.
- an annual review will be carried out

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using alerts and log files of internet traffic and web access
- individual device monitoring through software or third-party services
- any alerts are sent via email to the DSL who will check, deal with appropriately and record on a spreadsheet to evidence.

At Brunel College we use :

Messaging/commenting systems (incl. email, learning platforms & more)

Authorised systems

- Students at this school communicate with each other verbally and on social media. Student and staff communication is mostly verbally. Students have an email account that is configured on their iPads and can also be setup on their own devices if needed. Staff and students can email each other and email is sometimes used to help students practice their literacy.
- Staff at this school use the email system for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff are permitted to use this email system for any email communication that enables them to carry out their job.

- Staff also use WhatsApp to communicate. There is a whole staff WhatsApp group, an SLT WhatsApp group, an IT support WhatsApp group, with John Heagren from Wiltshire technology and others.

- RingCentral, a Voice Over IP service is used for making calls from staff mobile phones . Direct numbers are allocated to staff as needed. Staff can only make calls to parents and students as appropriate, via the Ring Central App.

- Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the Head Teacher and centrally managed.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles

- More detail for all the points below are given in the Social media section of this policy as well as the school's acceptable use agreements, behaviour policy and staff code of conduct.
- Appropriate behaviour is always expected, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be always followed when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.
- Pupils and staff are allowed to use the email system for reasonable personal use but should be aware that all use is monitored, their emails may be read, and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

Online storage or learning platforms

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc.

For all these, it is important to consider data protection and cybersecurity before adopting such a platform or service, and always, when using it. Brunel College is developing a clear cybersecurity policy and has a clear data protection policy which staff, governors and volunteers must follow at all times.

Passwords need to be strong and password hygiene is important for example the same password is not used for all systems. Staff must lock computers and devices, if they need to leave unattended. The use of Flash drives is strongly discouraged. Staff are encouraged to save files on Microsoft OneDrive or Microsoft SharePoint via MS Teams.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Trustees have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to Nicki Wright the school business manager.

The site is hosted by Wix. The School Business manager, SLT member for IT and Head teacher have access to edit the site. The network manager John Heagren has access, so that he can manage the forwarding from the Waspcentre.com and wascentre.org.uk domains to the Brunelcollege.co.uk domain .

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited, and material only used with permission.

Digital images and video

When a pupil/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. Parents answer as follows:

- For displays around the school
- For use in paper-based school marketing and or school prospectus
- For the school website
- For social media
- For paper based media – this may include local newspapers, promotional material or websites for external events/ competitions organisers in which students have participated.

Whenever a photo or video is taken/made, the member of staff will check that the student gives consent and will check the students records to see if there is permission to take photos.

Any pupils shown in public facing materials are never identified with their full name and first names will only be used in exceptional circumstances.

All staff are governed by their contract of employment and the school's Acceptable Use Agreement/ Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. Members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation. Photo must only be taken from the WASP PHOTO WhatsApp account and all staff must configure WhatsApp that photos are NOT automatically downloaded.

Staff and parents are regularly reminded 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.

We encourage young people to think about their online reputation and digital footprint, so we should be 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).

Pupils are taught about how images can be manipulated in their online safety education programme and taught to consider how to publish for a wide range of audiences which might include Trustees, parents or younger children.

Pupils 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.

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 / or a friend are subject to bullying or abuse.

Social media

Our SM presence

Brunel College works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first Googling the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve school (and staff) online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Zoe Hibberd is responsible for managing our Facebook and Instagram accounts.

Staff, pupils' and parents' SM presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the Acceptable use Agreement (all members of the school community sign), we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as avoiding any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+). We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

However, the school needs to strike a difficult balance of not encouraging underage use, at the same time as needing to acknowledge reality, in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when. Late at night/ in bedrooms is not helpful for a good night's sleep and productive learning at school the next day. You may wish to refer to the IWF website for ground rules https://talk.iwf.org.uk/agree-ground-rules/ or LGfL website https://parentsafe.lgfl.net/#h.7pzzapffhj9q to help establish shared

expectations and the Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

Although the Brunel College has an official Facebook and Instagram accounts we ask that parents/carers do not use these channels to communicate with the school, especially not to communicate about their children.

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

Pupils/students are not allowed to be 'friends' with or make a friend request to any staff, Trustees, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, Trustee, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUA's. However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher and should be declared upon entry of the pupil or staff member to the school.

Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions must not be attributed to the school, trustees or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a significant number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school AUA on Digital images and video. Permission should be sought before uploading photographs, videos or any other information concerning other people.

The statements of the Acceptable Use Agreement (AUA's) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Device usage

AUA's remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUA's and the sections of this document which impact upon

device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology and bring your own device (BYOD)

- **Students** are allowed to use mobile phones during lunch and break times. During lesson times phones should be handed in to a member of staff and are then held securely at reception.
- **Volunteers, contractors, trustees** should leave their phones in their pockets. Under no circumstances should they be used in the presence of students to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Business Manager must be sought.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children.
- **Staff** communicate using their mobile phones and there is dedicated WhatsApp group that staff can use to take photos for example of student work. Staff must disable automatic downloading of images from WhatsApp so these photos are not stored on staff devices.

Use of school devices

Staff and pupils are expected to follow the terms of the school AUA for appropriate use and behaviour when on school devices, whether on site or at home.

School devices are not to be used in any way which contravenes AUA's, Behaviour Policy / Staff Code of Conduct.

WiFi is accessible to staff for their school and own devices (e.g. smartphones and laptops). This is for school-related internet use and limited personal use, within the framework of the Acceptable Use Agreement. This is monitored when staff are using the SCHOOL STAFF or SCHOOL DEVICES WiFi networks. The backup Internet connections via BT at the Main centre (Secure Guest WiFi) and Virgin Media at Boathouse Meadow (Boathouse Meadow WiFi) are unfiltered. Student devices are not connected to these networks.

School devices for staff and students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable as well as appropriate personal use. iPads are managed using Mosyle.

Each student has a dedicated iPad and this accesses the SCHOOL DEVICES network which has filtering in place through Co-connect. There is automatic monitoring via NetSweeper every minute and alerts are sent to the DSL and IT SLT member.

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 pupils/property on school premises. This includes the content of mobile phones and other devices, for example because 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

Brunel College, Online Safety Policy - 2023/4

Appendix – Roles

Please read the relevant roles & responsibilities section from the following pages.

All school staff must read the "All Staff" section as well as any other relevant to specialist roles

Roles:

- All Staff
- Headteacher
- Designated Safeguarding Lead
- Trustees led by Online Safety / Safeguarding Link Trustee
- PSHE / RSHE Lead
- Computing Lead
- Subject leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Pupils
- Parents/carers
- External groups including parent associations

All staff

All staff should sign and follow the staff Acceptable Use Agreement in conjunction with this policy, the school's main Safeguarding policy, the Code of Conduct and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the DSL as named in the AUA, maintaining an awareness of current online safety issues (see the start of this document for issues in 2023) and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about overblocking, gaps in provision or pupils bypassing protections.

Headteacher – Craig Noble

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding

- Oversee and support the activities of the DSL 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 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.
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with technical colleague and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
    - In 2023/4 this will involve starting regular checks and annual reviews, upskilling the DSL and appointing a filtering and monitoring Trustee.
- Liaise with the DSL 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 pupils in the home and remote-learning procedures, rules and safeguards.
- 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 trustees to ensure a 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 pupils, including risk of children being radicalised
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead / Online Safety Lead – Kerry Williams

Key responsibilities (remember the DSL can delegate certain online-safety duties but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

- The DSL should "take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place).
- Ensure "An effective whole school approach to online safety" as per KCSIE
- In 2023/4 working to take up the new responsibility for filtering and monitoring by working closely with technical colleagues, SLT and the new filtering Trustee to learn more about this area,

better understand, review and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home.

- Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.
    - In 2023/4 this must include filtering and monitoring and help them to understand their roles
    - all staff must read KCSIE Part 1 and all those working with children also Annex B – translations are available in 13 community languages at kcsietranslate.lgfl.net (B the condensed Annex A can be provided instead to staff who do not directly work with children if this is better)
    - cascade knowledge of risks and opportunities throughout the organisation
    - safecpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more
- Ensure that ALL 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 safeguarding 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 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 Agreements) 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.
- Promote an awareness of and commitment to online-safety throughout the school community, with a strong focus on parents, including hard-to-reach parents.

- Communicate regularly with SLT and the safeguarding Trustee/ Board 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 pupils to disclose issues when off site, especially when in isolation/quarantine, e.g. a survey to facilitate disclosures and an online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).

Trustees, led by Online Safety / Safeguarding Link Trustee – Morven Fletcher

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

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Undergo (and signpost all other 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
- Appoint a filtering and monitoring Trustee to work closely with the DSL on the new filtering and monitoring standards.
- 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
- Work with the DPO, DSL and headteacher to ensure a 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 and now also reminders about filtering and monitoring
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school or college approach to online safety with a clear policy on the use of mobile technology."

Brunel College, Online Safety Policy - 2023/4

PSHE Lead – Ali Marshall/ Kerry Williams

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE 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 pupils' lives."
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self evaluations, to capture progress" to complement the computing curriculum,
- Work closely with the DSL 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

Subject 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 RSHE curriculum, and model positive attitudes and approaches to staff and pupils 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/other technical support roles – John Heagren/Guy Griffith

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 when it comes to filtering and monitoring and in 2023/4 you will be required to support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the new DfE standards, protections for pupils in the home and remote-learning.
- 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 proceedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, 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.
- Ensure the data protection policy and future cybersecurity policy are up to date, easy to follow and practicable.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

Data Protection Officer (DPO) – Nicki Wright with support from One West

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cybersecurity policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

- Note that retention schedules for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Volunteers and contractors

Key responsibilities:

- Read, understand, sign and adhere to an Acceptable Use Agreement (AUA)
- Report any concerns, no matter how small, to the DSL.
- 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 our AUA, 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 pupil. The same applies to any private/direct communication with a pupil.

Students

Key responsibilities:

Read, understand, sign and adhere to the student/pupil AUA.

Parents/carers

Key responsibilities:

- Read, sign and adhere to the school's parental AUA, read the pupil AUA and encourage their children to follow it.