Bilborough College Online Safety Policy – July 2024

Introduction

Key people / dates

	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Michelle Harvey
	Deputy Designated Safeguarding Leads / DSL Team Members	Monique Norcliffe Helen Ginns-Farrow
	Link governor for safeguarding and web filtering	Chris Hulse, Sharon Jagdev Powell
	Other staff member with relevance to online safeguarding and their role,	
	Network manager / other technical support	James Talbot Jason Wilson
	Date this policy was established and by whom	Autumn 2024 Michelle Harvey
	Date of next review and by whom To be reviewed biannually	Autumn 2026 Michelle Harvey

What is different about this policy?

In September 2023, changes to KCSIE have been made to reflect trends seen over the past year, the most significant change relating to filtering and monitoring. The DSL now takes lead responsibility for web filtering and monitoring, marking a clear shift. Colleges now need to follow the new DfE standards and consider the roles and responsibilities of all staff – for DSLs and SLT, the challenge is to better understand, review and drive the rationale behind decisions in this area. IT teams and safeguarding teams will need to work much more closely together for this to be possible and IT will be charged to carry out regular checks and feed back to DSL teams. All staff need to be aware of the changes and renewed emphasis and play their part in feeding back about over-blocking or gaps in the filtering provision. Colleges will also be reviewing their approaches to monitoring in line with the standards (note that filtering and monitoring are not the same – there is guidance around this at https://safefiltering.lgfl.net There is also training available via National Online Safety: Filtering and Monitoring (Secondary)

What is this Policy?

Online safety is an integral part of safeguarding and requires a whole college, cross-curricular approach, and collaboration between key college leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE). Any issues and concerns with online safety must always follow the college's safeguarding procedures.

Bilborough College Online Safety Policy – July 2024

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the college and local area.

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

Current Online Safeguarding Trends

In college 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: Our monitoring system and reported safeguarding incidents indicate online event types which include suicide, sexual content, cyberbullying, and vulnerable person. Many of the event reports from our monitoring system were students researching for their A level subject. All safeguarding event reports are taken seriously, where necessary external referrals are made, sanctions, intervention/s and/or support are actioned. These event types are discussed during preparatory meetings with the Lead Skills and Progression Teacher, who is responsible for developing the SOW for the Skills and Progression Programme, this informs revision of the SOW. All trends are included in the annual safeguarding report to governors, and this is shared with all staff.

Nationally, some of the latest trends of the past twelve months are outlined below.

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 college. 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.

The continued cost-of-living crisis has meant that young people 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 college we recognise that many of our 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.

PRIMARY SCHOOLS: 20% of 3–4-year-olds have access to their OWN mobile phone (let alone shared devices), rising to over 90 percent by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3 to 6 year olds are being tricked into 'self-generated' sexual content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home and the 7-10 year old age group is the fastest growing for this form of child sexual abuse material, up 60 percent within 12 months to represent over 60,000 cases found (of this same kind where the abuser is not present).

Bilborough College Online Safety Policy – July 2024

SECONDARY SCHOOLS: 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 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 colleges have had to counter.

Over the past year, there was a marked increase in the number of colleges 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 colleges).

There has been a significant increase in the number of fake profiles causing issues in colleges, both for colleges – where the college 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).

This policy is available.

- On the college website
- Part of college induction for <u>all</u> new staff (including temporary and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff.
- Reflected in the Acceptable Use Policies, which is signed or agreed by all when logging onto a college owned device.

Contents

Bilborough College Online Safety Policy – July 2024

Bilborough College Online Safety Policy – July 2024

Overview

Aims

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

- Setting out expectations for all Bilborough 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., Skills and Progression Programme) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the college gates and college 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 young people for the risks and opportunities of todays and tomorrow's digital world, to survive and thrive online.
- Helping college staff working with young people to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the 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 college, supporting the college ethos, aims and objectives, and protecting the reputation of the college 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 college policies such as Student Disciplinary Policy, Protection for Students from Child-on-Child Abuse (Bullying and Harassment) at College, Student Agreement and Code of Conduct)

Further Help and Support

Internal college channels should always be followed first for reporting and support, as documented in college policy documents, especially in response to incidents, which should be reported in line with your Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs MASH and the DSL/Principal/Director of HR will handle referrals to the LA designated officer (LADO).

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both students 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/carers, and anonymous support for young people. Training is also available via **safetraining.lgfl.net**

Bilborough College Online Safety Policy – July 2024

Scope

This policy applies to all members of the Bilborough College community (including teaching, supply and support staff, governors, volunteers, contractors, 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 college role.

Roles and responsibilities

This college 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 college, and to immediately report any concerns or inappropriate behaviour, to protect staff, students, families, and the reputation of the college. 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 college 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 student, 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 colleges establish a carefully sequenced curriculum for online safety that builds on what students 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 students navigate the online world safely and confidently regardless of the device, platform, or app.

The Skills and Progression Programme have the clearest online safety links, which include students' online reputation, radicalisation etc.

However, it is the role of all staff to identify opportunities to thread online safety through all college activities, both outside the classroom and within the curriculum and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology (devices, the internet, innovative technology such as AI artificial intelligence, AR augmented reality, etc) in college or setting as a homework task, all staff should encourage sensible use, monitor what students are doing, consider age appropriateness of websites. Ask DSL what appropriate filtering and monitoring policies are in place.

All staff should carefully supervise and guide students when engaged in learning activities involving online technology involving online technology, 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, parents, and carers.

Bilborough College Online Safety Policy – July 2024

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should talk to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the corridors, toilets, and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

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

- Safeguarding Policy
- Protection for Students from Child-on-Child Abuse (Bullying and Harassment) at College Policy
- Student Disciplinary Policy
- Student Agreement
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- BFMAT Data Protection Policy
- Privacy Notice
- ICT Security Policy
- ICT and Cyber Security

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

Any suspected online risk or infringement should be reported to the online designated safeguarding lead, principal, or deputy principal 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 principal, deputy, unless the concern is about the Principal in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline 0800 028 0285

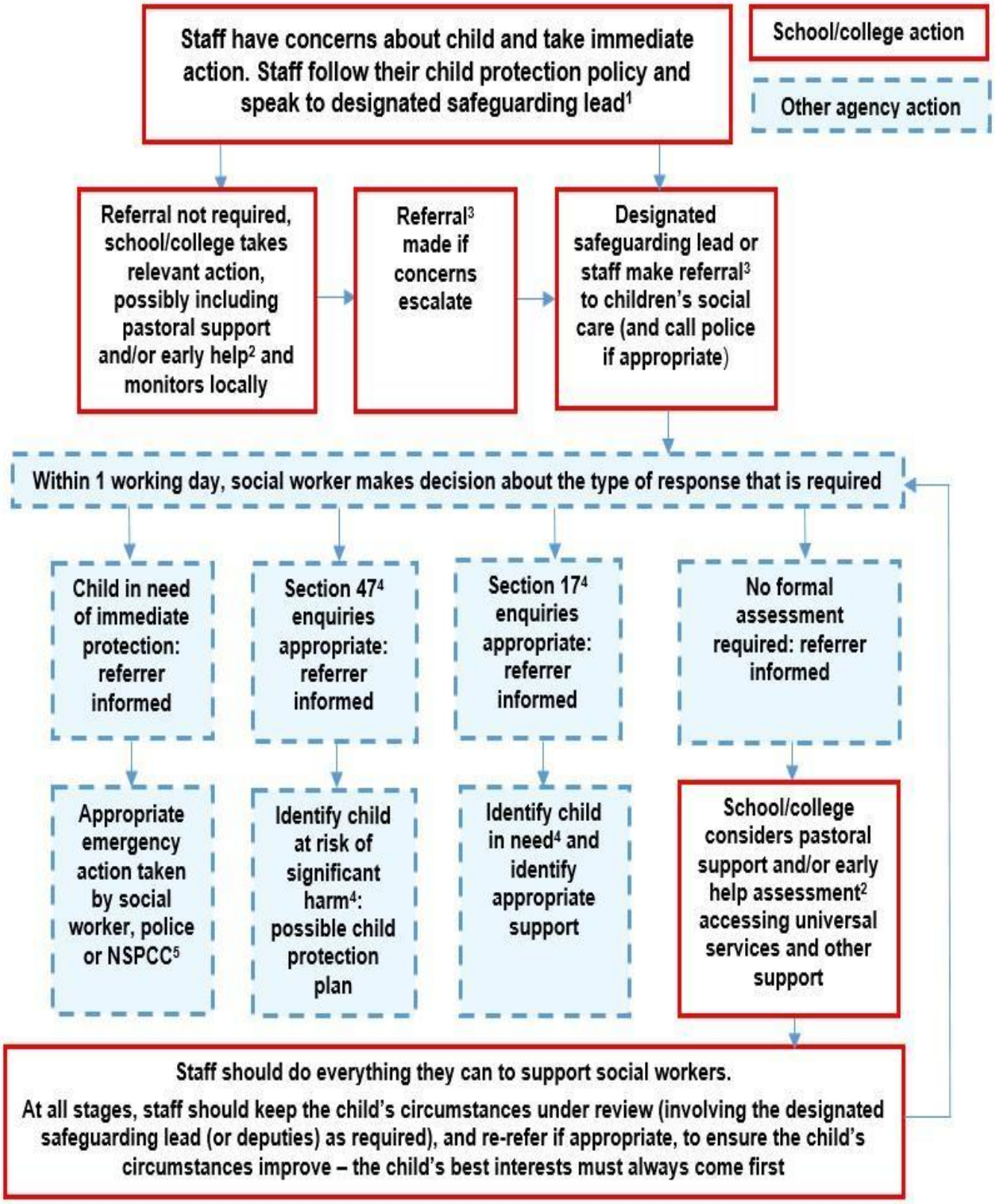
The college will actively seek support from other agencies as needed (i.e., the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2022 provides advice and related legal duties including support

for students 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 young person, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly concerning or breaks the law (procedures are in place for sexting and upskirting; see section below).

Actions where there are concerns about a child.

The following flow chart is taken from page 22 of Keeping Children Safe in Education 2023 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

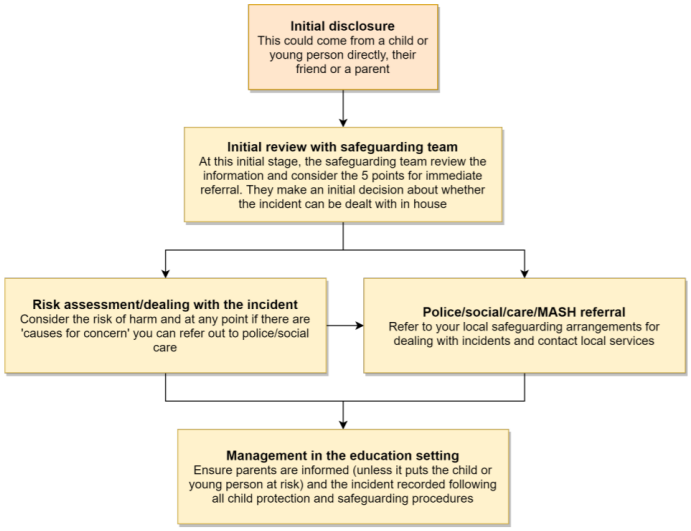

Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2] and monitors locally
Referral[3] made if concerns escalate
Designated safeguarding lead or staff make referral[3] to children's social care (and call police if appropriate)
Within 1 working day, social worker makes decision about the type of response that is required
Child in need of immediate protection: referrer informed
Section 47[4] enquiries appropriate: referrer informed
Section 17[4] enquiries appropriate: referrer informed
No formal assessment required: referrer informed
Appropriate emergency action taken by social worker, police or NSPCC[5]
Identify child at risk of significant harm[4]: possible child protection plan
Identify child in need[4] and identify appropriate support
School/college considers pastoral support and/or early help assessment[2] accessing universal services and other support
Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

Sexting – sharing nudes and semi-nudes.

All colleges (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 young people. 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 college 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 young person 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, students can come and talk to members of staff if they have made a mistake or had a problem in this area.

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 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 college or from home should be treated like any other form of bullying and the college bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter. Protection-for-Students-from-Child-on-Child-Abuse-Bullying-and-Harassment-at-College-Policy-August-2023.pdf (bilborough.ac.uk)

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 young people 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-college response; case studies are also helpful for training.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL/DDSL 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 colleges 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.

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

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

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of college platforms/networks/clouds, devices, and other technology.

Where students contravene these rules, the college Student Disciplinary policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

It will be necessary to reinforce these as usual at the beginning of any college year but also to remind students 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 college reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto college property.

The new responsibilities for filtering and monitoring, led by the DSL and following the new DfE standards, may mean that more such incidents will be discovered in future.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for young people and adults in the Bilborough community. These are also governed by college Acceptable Use Policies and the college social media policy.

Breaches will be dealt with in line with the student disciplinary policy (for students) 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 college community, Bilborough 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 college 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 students, staff, governors, volunteers, contractors, parents, and carers are bound by the college's BFMAT data protection and cybersecurity policy. It is important to remember that there is a close relationship between both data protection and cybersecurity and a college's ability to effectively safeguard young people. Colleges are reminded of this in KCSIE which also refers to the DfE Standards of Cybersecurity for the first time in 2023.

Colleges 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 colleges 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).

Colleges 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.

As colleges get to grips with these new standards, the challenge for DSLs and SLT is to better understand, review and drive the rationale behind decisions in this area. Tech teams and safeguarding teams will need to work much more closely together for this to be possible and technicians will be charged to carry out regular checks and feed back to DSL teams.

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 by email or speaking to a member of the safeguarding team and will be asked for feedback at the time of the regular checks which will now take place.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

It is important that colleges 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. (safetraining.lgfl.net)

At Bilborough College:

- web filtering is provided by Lightspeed on college site and for college devices used in the home.
- changes can be made by the IT helpdesk.
- overall responsibility is held by the DSL with further SLT support from the Deputy Principal
- technical support and advice, setup and configuration are from the James Talbot and Jason Wilson
- regular checks are made half termly by James Talbot and Jason Wilson to ensure filtering is still active and functioning everywhere. These are evidenced in a spread sheet owned by DSL, James Talbot, and Jason Wilson
- an annual review will be carried out as part of the online safety audit.

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
- network monitoring using log files of internet traffic and web access.
- individual device monitoring through software or third-party services

At Bilborough College, we use Lightspeed Systems to filter and monitor all college devices, college platforms and college WIFI for the purpose of safeguarding. BYODs are monitored when using the college WIFI and college platforms at home and in college.

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

Authorised systems

- Staff at this college use the email system provided by Microsoft Outlook for all college emails. They **never use a personal/private email account or other personal/private messaging platform** to communicate with young people or parents/carers, or to colleagues when relating to college/student data, using a non-college-administered system.

- Staff who create a social media account to represent the college (i.e., one which includes the word Bilborough / Bilbs / etc. in the title and is clearly a college account) must tag the main Bilborough account into every post and allow the college account to 'follow' their posts. Staff can use professional platform for students who have left etc for example LinkedIn.

Any systems above are centrally managed and administered by the college 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, students, and parents/carers, supporting safeguarding

best-practice, protecting young people against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any student login or storing college/student data must be approved in advance by SLT 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 student) or to the Principal/Deputy Principal (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 a private account is used for communication or to store data by mistake, the DSL/Principal/Deputy Principal/DPO (the 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 college's acceptable use agreements, student disciplinary 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 college into disrepute or compromise the professionalism of staff.
- Data protection principles will always be followed when it comes to all college communications, in line with the college Data Protection Policy and only using the authorised systems mentioned above.
- Students and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read, and the same rules of appropriate behaviour always apply. 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 college 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 always adopting such a platform or service and when using it. Bilborough College has a clear cybersecurity and data protection policy which staff, governors and volunteers must always follow.

College website

The college website is a key public-facing information portal for the college community (both existing and prospective stakeholders) with a key reputational value. Director of Planning and Operations have

delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to Marketing and the Clerk to the LGB

Where staff submit information for the website, they are asked to remember that colleges have the same duty as any person or organisation to respect and uphold copyright law – colleges have been fined thousands of pounds for copyright breaches. Sources must always be credited, and material only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected. If in doubt, check with a member of SLT.

Digital images and video

All images/videos that we collect are held securely held by the college and treated as confidential. If these are used for promotional marketing purposes, we do so based on our legitimate business interest to promote and market the college to perspective students.

All staff are governed by their contract of employment and the college's policies and training, which cover the use of mobile phones/personal equipment for taking pictures of students, and where these are stored. No member of staff will ever use their personal phone to capture photos or videos of students.

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).

Students are advised to be incredibly 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.

Social media

Our SM presence

Bilborough College works on the principle that if we do not 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 college online). Few parents/carers will apply for a college place without first Googling the college, 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 colleges' (and staff members') online reputation.

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

Daniel Cowlishaw and Nicola Kirby are responsible for managing our X-Twitter/Threads/Facebook/and other social media accounts and checking our Wikipedia and other mentions online. However, it is an ALL-STAFF responsibility to report any issues or concerns they identify.

Staff, Students,' and parents/carers' 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 college, we accept that many parents/carers, staff, and students will use it. However, as stated in the acceptable use policies which all members of the college community sign, we expect everybody to behave in a positive manner, engaging respectfully with the college and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the college 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/carers have a concern about the college, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the college complaints procedure should be followed, please follow this LINK to our policies. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, students, and parents/carers, also undermining staff morale and the reputation of the college (which is important for the students we serve).

Young people often learn most from the models of behaviour they see and experience, which will often be from adults. Parents/carers can support their young person by talking to them about the apps, sites, and games they use, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at college the next day). You can refer to the Digital Family Agreement 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 college has an official Facebook/Twitter account and will respond to general enquiries about the college, it asks parents/carers not to use these channels, especially not to communicate about their young people.

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

Students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers, and contractors or otherwise communicate via social media.

Students are discouraged from 'following' staff, governor, volunteer, or contractor public accounts (e.g., following a staff member with a public Instagram account) as laid. 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/Principal and should be declared upon entry of the student or staff member to the college).

** 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 college 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 college or its stakeholders on social media and be careful that their private opinions might not be attributed to the college, trust, or local authority, bringing the college into disrepute.

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

All members of the college community are reminded that particularly in the context of social media, it is important to comply with the college policy on Digital images and video and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the college community agree to when accessing a college device, are also relevant to social media activity, as is the college's Data Protection Policy.

Device usage

AUPs remind those with access to college devices about rules on the misuse of college 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 AUPs 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.

- **Students** are allowed to bring mobile phones into college and may use mobile phones during lunch break, when moving around the college buildings. During lessons, phones must remain always turned off, unless the teacher has given express permission as part of the lesson. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will be dealt with in line with the student disciplinary policy and the withdrawal of mobile privileges. Important messages and phone calls to or from parents/carers can be made from the classroom.

- **All staff who work directly with young people** should leave their mobile phones on silent and only use them in private staff areas during college hours. See also the 'Digital images and video' section of this document and the college data protection cybersecurity policies. Student/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of young people or to take photographs or videos. If this is required (e.g., for contractors to take photos of equipment or buildings), permission of the principal/deputy principal should be sought (this may be delegated) and this should be done in the presence of a member staff.
- **Parents/carers** when at college events, please refer to the Digital images and video section of this document on page. Parents/carers are asked not to call students on their mobile phones during lesson time; urgent calls are permitted.

Use of college devices

Staff and students are expected to follow the terms of the college acceptable use policies for appropriate use and behaviour when on college devices, whether on site or at home.

College devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct.

Wi-Fi is accessible for use of BYOD, guest networks and other college related internet use. All such use is monitored.

College devices for staff or students are restricted to the apps/software installed by the college, whether for use at home or college, and may be used for learning and reasonable as well as appropriate personal use.

For safeguarding purposes, all, and any usage of devices and/or systems and platforms may be tracked.

Trips / events away from college

For college trips/events away from college, teachers will be issued a college duty phone and this number used for any authorised or emergency communications with students and parents/carers. Any deviation from this policy (e.g., by mistake or because the college phone will not work) will be notified immediately to the principal/deputy principal. 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 college 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 college's search procedures are available in the college Physical intervention, Search and Safe Touch Policy and Procedure.

Bilborough College Online Safety Policy – July 2024

Appendix – Roles

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

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

Roles:

- All Staff
- Principal
- Designated Safeguarding Lead
- Governing Body, led by Online Safety / Safeguarding Link Governor
- Skills and Progression (SP) Lead/s
- Computing Lead
- Subject / aspect leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors
- Students
- External groups

All staff

All staff agree to the acceptable use policy (AUP) each time they log on to a college device. All staff will adhere to this online safety policy and should sign the staff HR declaration at the start of each year, to say they will do so,
the college's main safeguarding policy, the code of conduct and relevant parts of Keeping Children Safe in Education to support a whole-college safeguarding approach.

This includes reporting any concerns, no matter how small, to the designated safety lead as named in the AUP, 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 college 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 students bypassing protections.

Principal/Deputy Principal – David Shaw, Jane Beswick

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-college 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 college).
- 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 college's arrangements. *Bilborough College has procured online safety training on National Online Safety.*
- Ensure the college implements and makes effective use of appropriate ICT systems and services including college-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 colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE. LGFL's Safeguarding Shorts: Filtering for DSLs and SLT twilight provides an overview.
- In 2023/4 this will involve starting regular checks and annual reviews, upskilling the DSL, and appointing a filtering and monitoring governor.
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on college 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.
- Take overall responsibility for data management and information security ensuring the college's provision follows best practice in information handling; work with the DPO, DSL 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
- 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 young people being radicalised.
- Ensure the college website meets statutory requirements.

Designated Safeguarding Lead / Online Safety Lead – Michelle Harvey

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 college 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 governor 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. (https://lgfl.net/safeguarding/kcsie/web-filtering#appropriate)
- 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 students 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 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 (safetraining.lgfl.net)
- 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 young people 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 college)
- 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." – see safetraining.lgfl.net and prevent.lgfl.net
- 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 college trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter

- Ensure that online-safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider college life
- Promote an awareness of and commitment to online-safety throughout the college community, with a strong focus on parents/carers, including hard-to-reach parents/carers – dedicated resources at parentsafe.lgfl.net
- Communicate regularly with SLT and the safeguarding 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 college and for students to disclose issues when off site, especially when in isolation/quarantine, e.g. a survey to facilitate disclosures and an online form on the college home page about 'something that worrying me' that gets mailed securely to the DSL inbox
- Ensure staff adopt a zero-tolerance, whole college approach to all forms of child-on-child abuse, and do not dismiss it as banter (including bullying).

Governing Body, led by Online Safety / Safeguarding Link Governor – Chris Hulse and Sharon Jagdev Powell

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 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 – LGfL's Safeguarding Training for school governors is free to all college governors at safetraining.lgfl.net]
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated annually.
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards – there is guidance for governors at https://lgfl.net/safeguarding/kcsie/web-filtering
- Support the college in encouraging parents/carers 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 principal/deputy principal 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 college staff have read Part 1 of KCSIE; SLT and all working directly with young people 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 young people are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole college or college approach to online safety with a clear policy on the use of mobile technology."

Lead Skills and Progression Teachers (LSPT) – Emma Collins, Gemma Chapman

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 SP programme. "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.
- 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 student feedback opportunities.
- Work closely with the safeguarding team and all other staff to ensure an understanding of the issues, approaches, and messaging within SP programme.

Computing Lead – BFMAT IT Manager, James Talbot

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 LSPTs to avoid overlap but ensure a complementary whole-college approach.
- Work closely with the DSL 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 college to ensure a common and consistent approach, in line with acceptable use agreement.

Subject Leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, 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 Colleges 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 – Network and Cyber security engineer, Jason Wilson

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.
- Keep up to date with the college's online safety policy and technical information 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 college systems and networks reflect college 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 college's online security and technical procedures.
- To report online-safety related issues that come to their attention in line with college policy.

- Manage the college'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 cybersecurity policy are up to date, easy to follow and practicable.
- Monitor the use of college technology, online platforms, and social media and that any misuse/attempted misuse is identified and reported in line with college policy.
- Work with the Principal to ensure the college website meets statutory DfE requirements - see website audit tool at websiterag.lgfl.net

Data Protection Officer (DPO) – Data Protection Lead, Helen Dennis

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 young people 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 young people."
- Note that retention schedules 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. An example of an LA safeguarding record retention policy can be read at safepolicies.lgfl.net, but you should check the rules in your area.
- Ensure that all access to safeguarding data is limited as appropriate and monitored and audited.

Volunteers (including teaching)

Key responsibilities:

- Each time a person logs on to a college device they are agreeing to the acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible, and professional behaviours in their own use of technology at college 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 teaching session,** without the full prior knowledge and approval of the college, and will never do so directly with a student. The same applies to any private/direct communication with a student.

Bilborough College Online Safety Policy – July 2024

Students

Key responsibilities:

- Students click to say they agree to our acceptable use policy when they log onto a college device.

External groups – e.g., Mental Health Support Team and other supportive adults

Key responsibilities:

- Any external individual/organisation must click to say they agree to our acceptable use policy when they log onto a college device
- Support the college 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 from the DPO or DSL and refrain from posting negative, threatening, or violent. comments about others, including the college staff, volunteers, governors, contractors, students, or other parents/carers