Reaseheath College Online Safety Policy

Introduction

Key people / dates

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Paul Spearritt (Vice Principal Curriculum and Quality)
Deputy Designated Safeguarding Leads / DSL Team Members	Mark Birkitt (Head of Student Services) Kay Murray (Safeguarding Manager) Joanne Kavanagh (Head of Inclusive Learning) John Kendal (Assistant Principal Student Experience)
Link governor for safeguarding	Mike Gorton
Link governor for web filtering	Mike Gorton
Curriculum leads with relevance to online safeguarding and their role	James Eagney – Assistant Principal Performance and Progress Emily Jewell – Progress and Personal Development Manager.
Network manager / other technical support	Gareth Ferris – IT Systems and Infrastructure Manager Phil Ball – ICT Operations Manager
Date this policy was reviewed and by whom	Draft pending corporation approval as part of annual safeguarding report in term 1
Date of next review and by whom	October 26 – DSL

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' 2025 (KCSIE), 'Working Together to Safeguard Children 2023', 'Teaching Online Safety in Schools', statutory personal development guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Digital) and designed to sit alongside our Child Protection and Adult Safeguarding Policies. Any issues and

concerns with online safety **must** always follow the College's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

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. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, students and other stakeholders 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.

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 Personal Development will plan the curriculum for their areas, it is important that this ties into a whole-college approach.

What are the main online safety risks in 2025/2026?

Current Online Safeguarding Trends

In our 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, although seldom in frequency, which affect the wellbeing and safeguarding of our students:

- Attempts to access inappropriate websites, such as pornography and gambling.
- The sending of hateful online messages and images and online bullying.
- Sharing of inappropriate messages and images.
- Fake news and conspiracy theories.

Nationally, some of the latest trends of the past twelve months are outlined below. These are reflected in this policy and the acceptable use agreements we use, and seen in the context of the 4 Cs (see KCSIE for more details), a whole-college contextual safeguarding approach that incorporates policy and practice for curriculum, safeguarding and technical teams.

Last year, the rapid rise of generative AI (GenAI) was highlighted. Since then, the trend has exploded. Thousands of sites now offer AI-generated content, including disturbing levels of abusive, pornographic, and even illegal material like child sexual abuse content. Some platforms host AI "girlfriends," unregulated therapy bots, and even chatbots that encourage self-harm or suicide—tools many students can access freely at home or college. Chatbots can also blur reality, offering harmful advice or engaging in sexualised and bullying conversations. Their addictive design and unmoderated nature heighten the risk of overuse and exploitation.

When used for generating text, GenAI presents multiple risks. It can spread misinformation, facilitate plagiarism, and most worryingly, bypass safety settings. Many tools lack effective age controls and produce inappropriate content.

Beyond text, GenAI makes it easier than ever to create sexualised images and deepfake videos. These can have a devastating emotional and physical impact on young people, including blackmail and abuse. The Internet Watch Foundation has warned of a sharp rise in AI-generated child sexual abuse imagery. Alarming reports also show children using nudifying apps to create illegal content of peers.

AI searches involving sexualised and harmful content are on the increase. It's critical to stress that in the UK, *any* CSAM (child sexual abuse material)—AI-generated, photographic, or even cartoon—is illegal to create, possess, or share.

The college will address this through work in the classroom and through guidance to parents and students on the safe use at home.

Ofcom's 'Children and parents: media use and attitudes report 2025' has shown that YouTube remains the most used site or app among all under 18s, followed by WhatsApp, TikTok, Snapchat and Instagram. With children aged 8-14 spending an average of 2 hours 59 minutes a day online across smartphone, tablet and computer – with girls spending more time online than boys, four in ten parents continue to report finding it hard to control their child's screentime. Notably, 52% of 8-11s feel that their parents' screentime is also too high, underlining the importance of modelling good behaviour.

We have also come across online communications platforms that offer anonymous chat services and connect users with random strangers allowing text and video chats. Most of these are easily accessible to children on devices.

As a college 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 will 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 217,780 cases of self-generated child sexual abuse material were found of 11–13-year-olds (Internet Watch Foundation Annual Report 2025). These were predominantly (but importantly not only) girls; it is important also to recognise the increasing risk of financial sexual extortion, sometimes referred to as 'sextortion', where older teenage boys have been financially exploited after being tricked into sharing intimate pictures online. This resulted in the National Crime Agency releasing new guidance to all schools in Summer 2025.

Growing numbers of children and young people are using social media and apps, primarily TikTok as their source of news and information, with little attention paid to the facts or veracity of influencers sharing news.

There have also been significant safeguarding concerns where parents have filmed interactions with staff outside education premises and posted this on social media, putting children and the wider school community at risk of harm.

Research has shown that there was a marked increase in the number of education settings 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.

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

Cyber Security is an essential component in safeguarding children and now features within KCSIE. Sadly, the education sector remains a clear target for cyber-attacks.

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 our website.
- Part of the College's induction pack for all new staff (including casual and non-classroom-based staff and those starting mid-year).
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies.

Contents

Overview

Aims

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

- Setting out expectations for all Reaseheath 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. Personal Development) 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 campus 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 students for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Helping college staff working with students to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the students 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 Conduct Policy or Learner Harassment and Bullying Policy and Procedure).

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 the Child Protection and Safeguarding Policy and Safeguarding Adults Policy. The DSL (or DDSL) will handle referrals to local authority Child Protection Safeguarding Children Partnership and normally the Director of People and Culture will handle referrals to the LA designated officer (LADO). The college will work closely with the local authority, to seek advice and general support where appropriate.

The college will also utilise external support and helplines, where appropriate, 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 and anonymous support for children and young people.

Scope

This policy applies to all members of the Reaseheath College community (including teaching, casual staff, governors, volunteers, contractors, students/students, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their 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 post-16 study, 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. All staff have a key role to play in feeding back on potential issues.

Education and curriculum

It is important that the college establishes a carefully considered programme 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, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms provides an understanding of these risks to help tailor teaching and support to the specific needs of students, including vulnerable students.

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, supporting curriculum leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for students).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in college or setting as homework tasks, all staff should encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation and fake news), access to appropriate materials and signposting, and legal issues such as copyright and data law.

At Reaseheath College we recognise that online safety and broader digital resilience must be thread throughout the curriculum. We utilise our Career Ready programme to deliver many of the key

requirements associated with Online Safety, whilst also supporting staff to embed key elements in their everyday teaching and learning.

Annual reviews of curriculum plans / schemes of work (including for SEND students) are used as an opportunity to ensure that these key areas are being addressed and opportunities are not list. This is done within the context of an annual online safety audit, which is a collaborative effort led by the college's Safeguarding Leads.

We communicate with parents and carers about how we support students with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and safeguarding is everyone's responsibility.

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 speak to the safeguarding lead with any concerns (no matter how small these seem) 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, students accommodation, 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 mostly detailed in the following policies (primarily in the first key document):

- Child Protection and Safeguarding Policy
- Safeguarding Adults Policy
- Learner Harassment and Bullying Policy and Procedure
- Acceptable Use Policies
- Prevent Risk Register
- Reaseheath Information Security Policy
- Data Processing and Lawful Basis / Data Protection and Photography

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 through the college's escalation processes.

Any suspected online risk or infringement should be reported to the DSL or member of the safeguarding leads team on the same day. The reporting member of staff will ensure that a record is made of the concern on CPOMS, this includes any concerns raised by the filtering and monitoring systems e.g. Lightspeed.

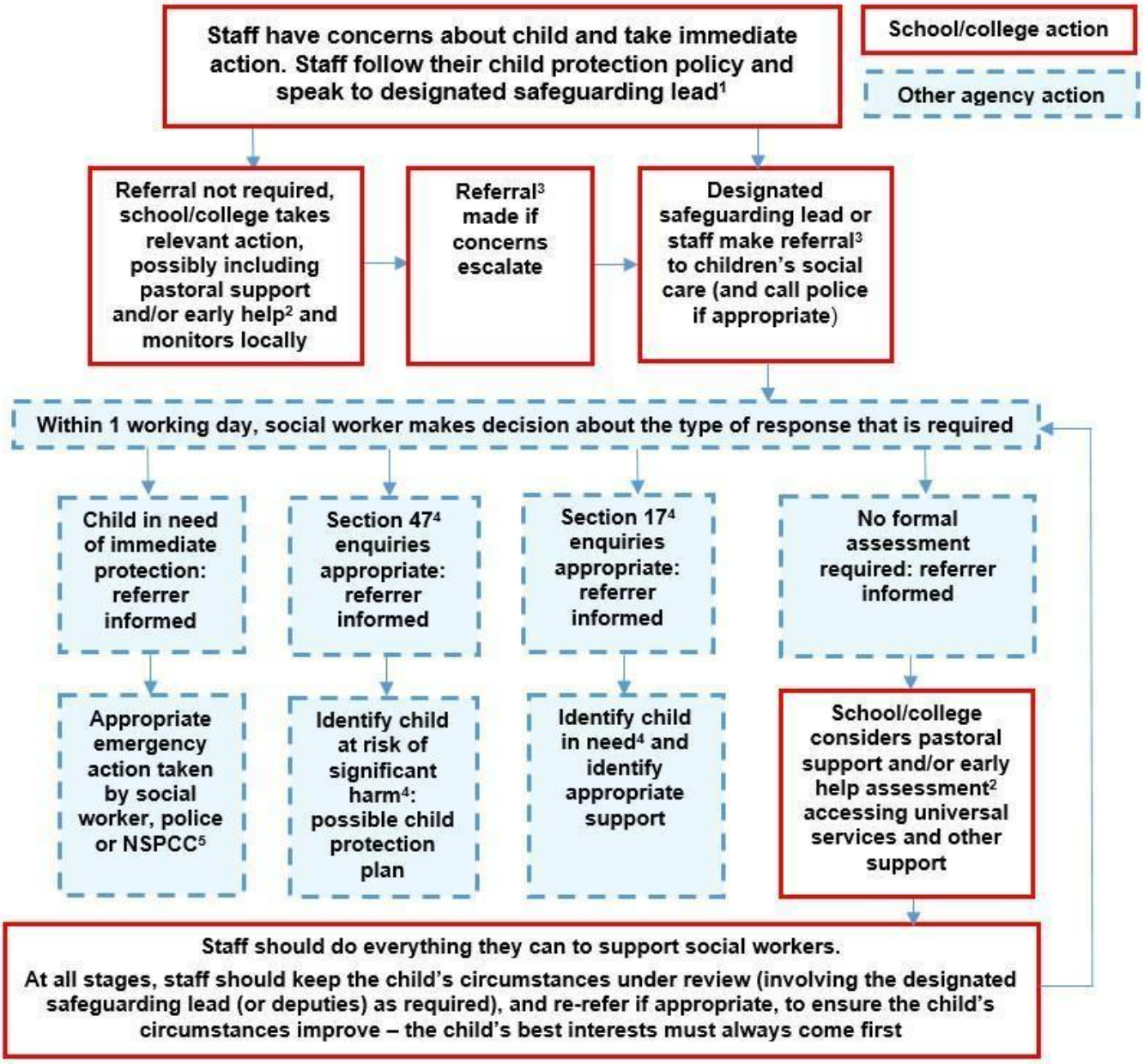
Any concern/allegation about staff misuse is always referred directly to the Director of People and Culture or DSL, unless the concern is about the Principal in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The college 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).

We will inform parents/carers of online-safety incidents involving their children, unless doing so would put them at risk, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

Actions where there are concerns about a child

The following flow chart is taken from page 24 of Keeping Children Safe in Education 2025 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

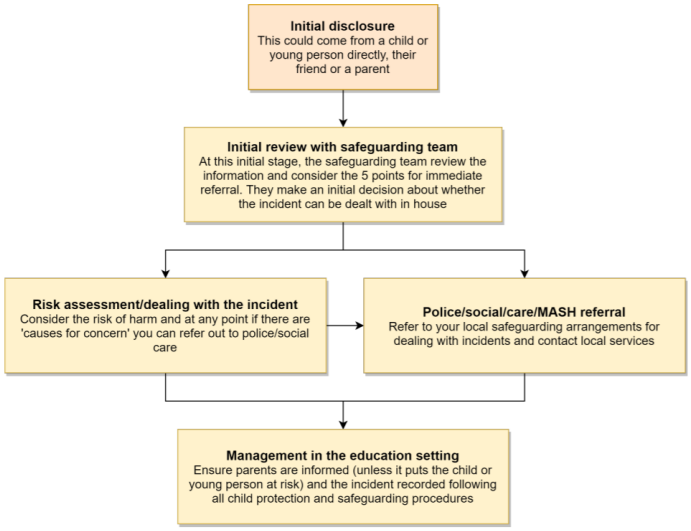
Nudes – sharing nudes and semi-nudes

The college refers to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings.

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.**

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, students should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

The 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 student 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

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 learner harassment and bullying policy and procedure 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 sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

Child-on-child sexual violence and sexual harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance in KCSIE. 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 Information Technology and Communications Acceptable Use Policy, Staff Social Media Policy and the Student Social Media 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's Student Conduct Policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff Disciplinary Policy.

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.

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.

Social media incidents

Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the relevant safeguarding policy. Other policies that govern these types of incident are the college's Acceptable Use Policies and the college's social media policies.

Breaches will be dealt with in line with the Student Conduct Policy or Disciplinary Policy 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, Reaseheath 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.

CCTV

The College has installed the CCTV system with the main aim of reducing the threat of crime, protecting the College property and ensuring the safety of all individuals. In order to accomplish this objective, the system will be used for the following purposes:

- for the prevention, reduction, detection and investigation of crime and other incidents
- to ensure the safety of staff, students and visitors
- assist with the identification, apprehension and prosecution of offenders
- to assist in the investigation of suspected breaches of College regulations by staff or students
- assist with the identification of actions that might result in disciplinary proceedings against staff and students
- monitor security of campus buildings
- the monitoring and enforcement of traffic related matters.

The CCTV system will be used to observe the College's campuses and areas under surveillance in order to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed

The College seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy. Further details can be found in the Reaseheath College CCTV Policy.

Extremism

The college has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the college, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Data protection and cybersecurity

All students, staff, governors, volunteers, contractors and parents are bound by the college's data protection policy and the Reaseheath College ICT Disaster Recovery Plan. 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 children. Colleges are reminded of this in KCSIE which also refers to the DfE Standards of Cybersecurity for Schools and Colleges.

Colleges should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child. And in KCSIE 2025, "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

The designated safeguarding lead (DSL) – Paul Spearritt - has lead responsibility for filtering and monitoring and works closely with IT Services to implement the DfE filtering and monitoring standards, which require colleges 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.

We look to provide appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times.

We ensure ALL STAFF are aware of filtering and monitoring systems 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 an email or Teams message to the DSL, or if appropriate a safeguarding concern via CPOMS, and will be asked for feedback at the time of the regular checks which 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 very 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.

Technical and safeguarding colleagues work together closely to carry out annual reviews and check and also to ensure that the college responds to issues and integrates with the curriculum.

We will carry out half-termly checks to ensure all systems are in operation, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc. More details of both documents and results are available on request from IT Services.

At our college we recognise that generative AI sites can pose data risks so staff are not allowed to enter child data and where they use them, they must be approved. For children and young people, we block the generative AI category and only allow specific sites. We know that what children input and what the tool outputs cannot be guaranteed as safe and inappropriate content can be generated, so we carefully monitor output and limit their use - also in line with DfE guidelines.

Safe Search is enabled via Cisco Umbrella, which then applied to all compatible search engines and YouTube.

Microsoft Edge is the only approved college browser available on college issued device.

DNS restrictions are in place and on, which provides moderate restriction for YouTube.

Out of hours, our policies are:

- Filtering and monitoring continue outside of core business hours for all college issued devices, via the Cisco Umbrella roaming client (All devices) and the Lightspeed Monitoring Agent (Student devices only). Alerts will continue to trigger and be sent to the relevant recipients at any point throughout the day. However, college staff may not be able to review/respond to these alerts outside of their normal working pattern.
- Cisco Umbrella is monitored 24/7 via an external SOC service (Security Operations Centre), dedicated contacts within the IT team will be notified of any suspicious activity related to filtering, via the SOC service.
- Similarly, the Lightspeed service contains 'Human Review', whereby an external team monitor alerts 24/7 from the Lightspeed Agent. They also have a dedicated safeguarding contacts list, to inform if specific incidents need to be highlighted.

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.

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

Reaseheath college procured Lightspeed Alert in 2023, to use as its monitoring system.

With Lightspeed Alert being cloud based, this allows devices at all Reaseheath sites (Main Campus, REAA) to be monitored using the same platform. Any college owned laptop used outside of the Reaseheath network will continue to benefit from monitoring, as the monitoring agent will report on specific keyword/image searches, regardless of location, provided the device in question is connected to the internet.

In addition, Lightspeed is also actively monitoring student Office 365 data, used in Teams, Outlook and OneDrive. This applies to any device a student accesses, whether college or personally owned.

The Lightspeed Alert dashboard provides critical information regarding alerts at a quick glance, providing our DSL and safeguarding team the ability to react in a timely manner and involve the relevant staff and third parties where required.

Lightspeed also include their 'Human Review Team', where alert cases are under constant review and anything deemed high risk (Based on the alert score), will also result in a phone call from the Lightspeed Human Review Team, to our DSL and/or safeguarding team.

The following categories are set by Lightspeed for alert data:

- Self-harm
- Bullying
- Explicit
- Violence
- Drugs
- Weapons

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

Authorised systems

- Students at this college communicate with each other and with staff using Office 365 tools including Outlook and MS Teams. In some curriculum areas, other learning platforms may be in use which enable students to send messages to each other and staff. ProMonitor is also used extensively to enable communication between staff and students. Communication via MS Teams will warn staff/students that the user email address attempting to contact them is outside of the Reaseheath.ac.uk domain.
- Staff at this college use the email system provided by Microsoft 365 for all college emails. They never use a personal/private email account to communicate with students or parents, or to colleagues when relating to college/student data, using a non-college-administered system. Staff are permitted to use this email system to communicate with all groups.

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, 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 the college and centrally managed. In the main, this is through the DPO and the Digital Strategy Group.

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 Director of People and Culture (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/Director of People and Culture/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles of messaging/commenting systems

- 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 conduct policy and staff code of conduct.
- Appropriate behaviour is expected at all times, 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 be followed at all times 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 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).

Use of generative AI

At Reaseheath College we acknowledge that generative AI platforms (e.g. ChatGPT or Bard for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the DfE's guidance on this. In particular:

- We will talk about the use of these tools with pupils, staff and parents – their practical use as well as their ethical pros and cons.
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, nudifying apps and inappropriate chatbots).
- The use of any generative AI in Exams, or to plagiarise and cheat is prohibited, and the Student Conduct policy will be used for any student found doing so.

- In college, we allow use of AI and provide students with guidance to support its use, specifically around when to use AI and when not to use AI. Use should be quoted and referenced accordingly.
- We support our staff to use generative AI to help with planning, and other elements of their role, via the use of Teachermatic.
- Any new platforms are requested via the Digital Strategy Group (or Executive in exceptional circumstances).

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 adopting such a platform or service and at all times when using it. Any new platforms will be approved by the Digital Strategy Group (or Executive in exceptional circumstances).

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. The Principal and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to the Head of Marketing.

The site is managed by / hosted by Face Interactive Limited.

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 the DPO.

Digital images and video

From time to time, photographs and videos are taken on and off campus as part of college life and for marketing, educational and promotional purposes. These images could be used in print and digital media formats including, print publications, websites, e-marketing, poster banners, advertising, film, social media, and for teaching and research purposes, etc. We do this to help showcase the work we do as an education provider and to support what our students are achieving.

When using images or recordings of people where individuals feature prominently and are clearly identifiable, a Consent Declaration is signed. The consent form is stored alongside the images for as long as the image/recording is retained.

All staff are governed by their contract of employment and the college's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of students, and where these are stored. At Reaseheath College staff are advised to use work phones to capture photos or videos of

students. Occasionally members of staff will use personal phones to capture content in instances where a work phone is unavailable, but these will be appropriate, linked to college activities, taken without secrecy and not in a one-to-one situation, and always moved to college storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos).

Photos are stored on SharePoint in line with the retention schedule of the college Data Protection Policy. Historic archive images are stored on the local network.

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

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 taught about how images can be manipulated in their Career Ready programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.

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

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

Social media

Our SM presence

Reaseheath 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 college online). Few students/parents 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 institutions' (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.

The Head of Marketing is responsible for managing our X-Twitter / TikTok / Facebook / Instagram / LinkedIn and other social media accounts and checking our Wikipedia, Trustpilot and Google reviews and other mentions online. All staff receive training on reporting content which may reflect negatively on the college as outlined in the Staff Social Media Policy.

Staff, students' 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 college, we accept that many parents, staff and students will use it. However, as stated in the acceptable use policies, 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 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. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, students and parents, also undermining staff morale and the reputation of the college (which is important for the students we serve).

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 college has 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 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 and young people 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 teaching and learning at college the next day).

Although the college has an official Facebook / X-Twitter / Instagram / TikTok / LinkedIn accounts and will respond to general enquiries about the college, it asks parents/carers not to use these channels, especially not to communicate about their children.

Email, and Teams, is the official electronic communication channel between parents 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). 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 student workers, pre-existing family links, but these 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 staff member) or to the Director of People and Culture (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 personal opinions might not be attributed to the college, bringing the college 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 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) are also relevant to social media activity, as is the college's Data Protection Policy.

Device usage

AUPs and the Data Protection and Photography policy 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.

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

- **Students** are allowed to bring mobile phones into college. During lessons, phones must remain on silent at all times and not used, unless the teacher has given express permission as part of the lesson, for example for multi-factor authentication. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to the initiation of the student conduct policy. The college can pass on messages from parents to students in emergencies.

- **All staff who work directly with students** 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 policies. Student/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** should leave their phones in their pockets and on silent. Under no circumstances should they be used in the presence of students or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Head of Estates should be sought, and this should be done in the presence of a member staff.
- **Parents** should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other students. When at college events, please refer to the Digital images and video section of this document on page.

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, student conduct policy / staff code of conduct.

Wifi is accessible to staff and students, and registered guests (via specific logins provided by IT Services) for college-related internet use / limited personal use within the framework of the acceptable use policy. 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 in college, and may be used for learning and reasonable as well as appropriate personal use.
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. Any deviation from this policy (e.g. by mistake or because the college phone will not work) will be notified immediately to the DSL. 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.

If on trips pupils are encouraged to connect to another organisation's Wi-Fi___33/network, staff must be aware that other connections may not be as well controlled (e.g. via filtering and monitoring) as the network and systems in college and therefore staff are responsible for risk assessing and managing such situations. Staff should seek advice from the DSL where necessary.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the 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 Student Substance Misuse Policy and the Offensive Weapons, Sharps and Bladed Articles Policy.

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 Safeguarding Link Governor
- Personal Development Lead
- Curriculum Area Manager & Tutors
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Students
- Parents/carers
- External groups

All staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the college's main safeguarding policy, the code of conduct/handbook 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 safeguarding lead, maintaining an awareness of current online safety issues (see the start of this document for issues in 2025) and guidance (such as KCSIE, 2025), 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 DfE standards for filtering and monitoring and play their part in feeding back to the DSL about overblocking, gaps in provision or pupils bypassing protections. All staff are also responsible for the physical monitoring of pupils' online devices during any session/class they are working within.

Principal

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 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.
- 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.
- 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 children being radicalised.
- Ensure the college website meets statutory requirements.

Designated Safeguarding Lead / Online Safety Lead

Key responsibilities

- 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.
- Ensure the college is complying with the DfE's standards on Filtering and Monitoring.
- As part of this, DSLs will work with technical teams to carry out reviews and checks on filtering and monitoring, to compile the relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant YouTube mode and preferred search engine/s etc.
- 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, 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.
    - 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
    - Cascade knowledge of risks and opportunities throughout the organisation.
- Ensure that ALL governors and 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 CMT, staff and technical colleagues to complete an online safety audit (including technology in use in the college).
- Work with the Principal, 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 Policies) and the strategy on which they are based (in harmony with policies for conduct, safeguarding, Prevent and others) and submit for review to the governors.
- Receive regular updates in online-safety issues and legislation, be aware of local and college trends.
- Ensure that online-safety education is embedded across the curriculum and beyond, in wider college life.
- Promote an awareness of and commitment to online-safety throughout the college community.
- Communicate regularly with CMT 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.
- Ensure staff adopt a zero-tolerance, whole college approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- Pay particular attention to any **online tutors**, that are engaged by the College.

Governing Body, led by Online Safety / Safeguarding Link Governor

Key responsibilities

- 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 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.
- 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 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; CMT 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.

Personal Development Lead

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 Personal Development 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. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their students' lives."
- Focus on the underpinning knowledge and behaviours to help students to navigate the online world safely and confidently regardless of their device, platform or app.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging.
- Work closely with all other lead staff to embed the same whole-college approach.

Curriculum Area Managers & Tutors

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your curriculum area and model positive attitudes and approaches to staff and students alike.
- Provide regular guidance to staff and students in the relevant curriculum area around online safety.
- Ensure department meetings, reviews etc cover online safety issues, along with other safeguarding updates.

IT Systems and Infrastructure Manager

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.
- Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as 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 DfE standard.
- Keep up to date with the college'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 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 other key policies are up to date, easy to follow and practicable.
- Monitor the use of college technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with college policy.

- Work with the DPO and Head of Marketing to ensure the college website meets statutory DfE requirements.

Data Protection Officer (DPO)

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, it's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child. And in KCSIE 2025, "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 student is aged 25 or older)'.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors (including tutor)

Key responsibilities:

- Adhere to an acceptable use policy (AUP).
- Report any concerns, no matter how small, to the designated safeguarding 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, 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.

Students

Key responsibilities:

- Read, understand, sign and adhere to the student charter.
- Adhere to relevant policies and procedures relating to online safety.
- Act on guidance provided by staff.
- Report any concerns to members of staff.

Parents/carers

Key responsibilities:

- Encourage their children to follow relevant policies and guidance, and support with their use.

External groups

Key responsibilities:

- Use technology or the internet in line with the acceptable use policy.
- 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 and refraining from posting negative, threatening or violent comments about others, including the college staff, volunteers, governors, contractors, students or other parents/carers.