Online Safety Policy

This policy has been approved by the Board of Trustees with reference to the academy's Equality Policy. The aims of the Equality Policy are to ensure that Plume Academy meets the needs of all, taking account of gender identity, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this academy we meet the diverse needs of students to ensure inclusion for all and that all students are prepared for full participation in a multi-ethnic society.

Author: Ash Stoneman, Vice Principal	**Ratified by Board of Trustees:** 20 September 2023
Last Reviewed: September 2023	**Next Review:** September 2024

Introduction

Key people / dates

Plume, Maldon's Community Academy 	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Mr Ash Stoneman (Vice Principal and DSL)
	Deputy Designated Safeguarding Leads / DSL Team Members	Mrs Ruth Clark (Alternative DSL) Mrs Kirsten D'Arcy Smith (Assistant DSL)
	Link Trustee for Safeguarding and Webfiltering	Mrs Denise Gray (Trustee for Safeguarding)
	Curriculum leads with relevance to online safeguarding and their role	Mr James Cooper (PD and RSE Lead)
	Network manager / other technical support	Mr Mark Beckett
	Date this policy was reviewed and by whom	September 2023
	Date of next review and by whom	September 2024

What is this policy?

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

Who is it for; when is it reviewed?

This policy should be a living document, subject to full annual review but also amended where necessary during the year in response to developments in the academy and local area. Although many aspects will be informed by legislation and regulations, we will involve staff, trustees, students and parents in writing and reviewing the policy and make sure the policy makes sense and it is possible to follow it in all respects. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Students could help to design a version in language their peers understand or help you to audit compliance. Acceptable Use Policies (see appendices) for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

Who is in charge of online safety?

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

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

Current Online Safeguarding Trends

In our academy 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: misuse of mobile phone technology, inappropriate sharing of images and the misuse of social media in various formats.

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

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

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

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

Against this background, the Ofcom 'Children and parents: media use and attitudes report 2023' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further. As an academy we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore remember to remind about best practice while remembering the reality for most of our students is quite different.

This is striking when you consider that over 95 percent of students have their own mobile phone by the end of Year 7, and the vast majority do not have safety controls or limitations to prevent harm of access to inappropriate material. This is particularly pertinent given that 130,556 cases of self-generated child sexual abuse material were found of 11-13 year olds (Internet Watch Foundation Annual Report). These

were predominantly (but importantly not only) girls; it is important also to recognise more and more older teenage boys being financially extorted after sharing intimate pictures online.

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

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

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

How will this policy be communicated?

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

- Posted on the academy website
- Part of academy induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, trustees, students and parents/carers (which must be in accessible language appropriate to these groups), which will be issued to whole academy community, on entry to the academy, annually and whenever changed, plus displayed in academy

Contents

Overview

Aims

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

- Setting out expectations for all Plume, Maldon's Community Academy community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the academy gates and academy day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Helping academy staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the academy, supporting the academy ethos, aims and objectives, and protecting the reputation of the academy 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 academy policies such as Behaviour Policy or Anti-Bullying Policy)

Further Help and Support

Internal academy channels should always be followed first for reporting and support, as documented in academy policy documents, especially in response to incidents, which should be reported in line with your Child Protection & Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the Joint Head of Academy will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

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, and anonymous support for children and young people. Training is also available via **safetraining.lgfl.net**

Scope

This policy applies to all members of the Plume, Maldon's Community Academy community (including teaching, supply and support staff, trustees, 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 academy role.

Roles and responsibilities

This academy 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 academy, and to immediately report any concerns or inappropriate behaviour, to protect staff, students, families and the reputation of the academy. 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 academy community should **read the relevant section in Annex A of this document** that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the annex.

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

Education and curriculum

It is important that academy's 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, Teaching Online Safety in schools recommends embedding teaching about online safety and harms through a whole academy approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of students, including vulnerable students – dedicated training around this with curriculum mapping for RSHE/PSHE and online safety leads is available at safetraining.lgfl.net

RSHE guidance also recommends academy's assess teaching to "identify where students need extra support or intervention [through] tests, written assignments or self evaluations, to capture progress."

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)

- Computing
- Citizenship

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all academy activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for students)

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

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

At Plume, Maldon’s Community Academy we recognise that online safety and broader digital resilience must be thread throughout the curriculum.

Annual reviews of curriculum plans / schemes of work (including for SEND students) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

https://www.plume.essex.sch.uk/personal-development-at-plume

This is done within the context of an annual online safety audit, which is a collaborative effort led by Mr Stoneman, the Vice Principal and Designated Safeguarding Lead.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship).

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 err on the side of talking 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 playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

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

- Safeguarding and Child Protection Policy
- Child-on-Child Abuse Policy
- Anti-Bullying Policy
- Behaviour Policy (including academy sanctions)
- Prevent Risk Assessment / Policy

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

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

Any concern/allegation about staff misuse is always referred directly to the Joint Head of Academy, unless the concern is about the Joint Head of Academy in which case the complaint is referred to the Chair of Trustees and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline (you may want to display a poster with details of this / other helplines in the staff room – see posters.lgfl.net and reporting.lgfl.net).

The academy will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2022 provides advice and related legal duties including support for 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 children, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly concerning or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

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

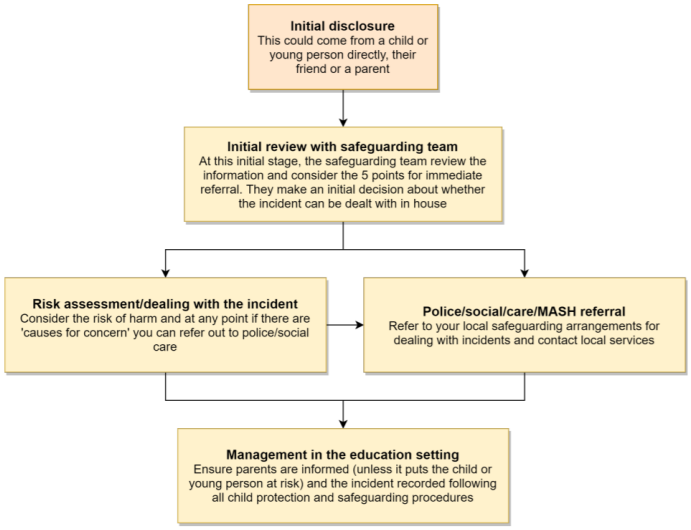
Sexting – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid

unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

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

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



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

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

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

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

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child on child abuse students/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 academy or from home should be treated like any other form of bullying and the academy bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

Please see our Anti Bullying policy below:

https://www.plume.essex.sch.uk/_files/ugd/03a94d_fba0a117b86e4a92a51ec2fd4a97f26f.pdf

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

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

Child-on-child sexual violence and sexual harassment

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

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

In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour.

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

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

Where students contravene these rules, the academy behaviour 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 academy 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 academy reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto academy 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 the coming year but the academy will do its best to remind students and staff of this increased scrutiny at the start of the year.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Plume, Maldon's Community Academy community.

Breaches will be dealt with in line with the academy behaviour policy (for students) or code of conduct/handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the academy community, Plume, Maldon's Community Academy 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 academy 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 and parents are bound by the academy's behaviour of parents and carers policy which can be found here.
https://www.plume.essex.sch.uk/_files/ugd/03a94d_4d295773773947bdb9c0d6213ccb0c50.pdf

It is important to remember that there is a close relationship between both data protection and cybersecurity and a schools ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cybersecurity for the first time in 2023.

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

Appropriate filtering and monitoring

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

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

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

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

As schools 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 via MyConcern – our safeguarding platform as an academy 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 regular training reminders in the light of the annual review and regular checks that will be carried out.

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

At Plume, Maldon's Community Academy

- web filtering is provided by WatchGuard on academy site and for academy devices used in the home
- changes can be made by ICT Support
- overall responsibility is held by the DSL
- technical support and advice, setup and configuration are from ICT Support
- regular checks are made half termly by ICT Support to ensure filtering is still active and functioning everywhere. These are evidenced using the SWGfL Filter Test (http://testfiltering.com/)
- an annual review is carried out as part of the online safety audit to ensure a whole academy approach, in line with onlinesafetyaudit.lgfl.net

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

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

Authorised systems

- Students at this academy communicate with each other and with staff using email on our Microsoft 365 email system
- Staff at this academy use the email system provided by Microsoft 365 email for all academy emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to academy/child data, using a non-academy-administered system. Staff are permitted to use this email system to communicate with all stakeholders.
- Staff at this academy use Microsoft 365 and InTouch SIMs to communicate with relevant stakeholders as required.

Any systems above are centrally managed and administered by the academy 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 children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any child login or storing academy/child data must be approved in advance by the academy and centrally managed by our Business and Estates Manager, Mr Scott.

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

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

Behaviour / usage principles

- More detail for all the points below are given in the Social media section of this policy as well as the academy's acceptable use agreements, behaviour 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 academy into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all academy communications, in line with the academy 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).

Online storage or learning platforms

All the principles outlined above also apply to any system to which you log in online to conduct academy 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. Plume, Maldon's Community Academy has a clear cybersecurity and data protection policy which staff, trustees and volunteers must follow at all times.

Academy website

The academy website is a key public-facing information portal for the academy community (both existing and prospective stakeholders) with a key reputational value. The Joint Head of Academy and Trustees have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to Mark Beckett, Director of ICT Systems.

The site is managed by ICT Support, and hosted by Wix.com

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

Digital images and video

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

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

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

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

All staff are governed by their contract of employment which covers the use of mobile phones/personal equipment for taking pictures of students, and where these are stored. At Plume, Maldon's Community Academy, no member of staff will ever use their personal phone to capture photos or videos of students or members of staff may occasionally use personal phones to capture photos or videos of students, but these will be appropriate, linked to academy activities, taken without secrecy and not in a one-to-one situation, and always moved to academy 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 the OneDrive in line with the retention schedule of the academy Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. Further detail on this subject and a sample letter to parents for taking photos or videos at academy events can be found at parentfilming.lgfl.net

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 online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

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

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

Social media

Our SM presence

Plume, Maldon's Community Academy 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 academy online). Few parents will apply for a academy place without first Googling the academy, 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 schools' (and staff members') online reputation.

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

Staff account holders are responsible for managing our Facebook/and other social media accounts and checking our Wikipedia and Google reviews and other mentions online.

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 an academy, we accept that many parents, staff and students will use it. However, as stated in the acceptable use policies which all members of the academy community sign, we expect everybody to behave in a positive manner, engaging respectfully with the academy 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 academy 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 academy, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the academy 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 academy (which is important for the students we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the academy regularly deals with issues arising on social media involving students/students under the age of 13. 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 academy 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/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at academy the next day). You may wish to 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 academy has an official Facebook account and will respond to general enquiries about the academy, it asks parents/carers not to use these channels, especially not to communicate about their children.

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

Students/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/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 pre-existing family links, but these must be approved by the Joint Head of Academy, and should be declared upon entry of the student or staff member to the academy).

** 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 Joint Head of Academy (if by a staff member).

Staff are reminded that they are obliged not to bring the academy 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 academy or its stakeholders on social media and be careful that their personal opinions might not be attributed to the academy, trust or local authority, bringing the academy 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 academy community are reminded that particularly in the context of social media, it is important to comply with the academy policy and permission is sought before uploading photographs, videos or any other information about other people.

Device usage

AUPs remind those with access to academy devices about rules on the misuse of academy 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 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)

- **Mill Road Campus Students/students** are allowed to bring mobile phones in for emergency use only. During lessons, phones must remain turned off at all times. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to Behaviour Policy being utilised and the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the academy office, which will also pass on messages from parents to students in emergencies.
- **Fambridge Road Campus Students/students** are allowed to bring mobile phones in for emergency use only / may use mobile phones during breaks and lunch breaks, but not when moving around the academy buildings. During lessons, phones must remain turned off at all times, 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 lead to our Behaviour Policy being utilised and the withdrawal of mobile privileges. Important messages and

phone calls to or from parents can be made at the academy office, which will also pass on messages from parents to students in emergencies.

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during academy hours. See also the 'Digital images and video' section of this document and the academy data protection cybersecurity policies. Child/staff data should never be downloaded onto a private phone.

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

- **Parents/Carers** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at academy events, please refer to the Digital images and video section of this document. Parents/Carers are asked not to call students on their mobile phones during the academy day; urgent messages can be passed via the academy office.

Use of academy devices

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

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

Wifi is accessible to guests for academy-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.

Academy devices for staff or students are restricted to the apps/software installed by the academy, whether for use at home or academy, 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 academy

For academy trips/events away from academy, teachers will be issued an academy duty phone and this number used for any authorised or emergency communications with students/students and parents. Any deviation from this policy (e.g. by mistake or because the academy phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will

ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Joint Head of Academy and staff authorised by them have a statutory power to search students/property on academy 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 academy's search procedures are available in the academy Behaviour Policy.

Appendix – Roles

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

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

Roles:

- All Staff
- Joint Head of Academy
- Designated Safeguarding Lead
- Board of Trustees, led by Online Safety / Safeguarding Link Trustee
- PSHE / RSHE Lead/s
- Computing Lead
- Subject / aspect leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Students
- Parents/carers
- External groups including parent associations

All staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the academy's main safeguarding policy, the code of conduct/handbook and relevant parts of Keeping Children Safe in Education to support a whole-academy safeguarding approach.

This includes reporting any concerns, no matter how small, to the designated safety lead as named in 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 academy 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.

Joint Head of Academy – Mrs Ruth Clark

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-academy 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 academy)
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL trustees undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that trustees are regularly updated on the nature and effectiveness of the academy's arrangements
- Ensure the academy implements and makes effective use of appropriate ICT systems and services including academy-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.
    - 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 academy 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 academy'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 academy website meets statutory requirements

Designated Safeguarding Lead / Online Safety Lead – Mr Ash Stoneman

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 academy 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.

- 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 trustees undergo safeguarding and child protection training (including online-safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online-safety and behaviour apply
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the academy)
- Work with the Joint Head of Academy, 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 academy 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 academy life
- Promote an awareness of and commitment to online-safety throughout the academy community, with a strong focus on parents, including hard-to-reach parents – 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 academy 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 academy home page about 'something that worrying me' that gets mailed securely to the DSL inbox
- Ensure staff adopt a zero-tolerance, whole academy approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- Pay particular attention to **online tutors**, both those engaged by the academy as part of the DfE scheme who can be asked to sign the contractor and those hired by parents.

Board of Trustees Body, led by Online Safety / Safeguarding Link Trustee – Denise Gray

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 academys and colleges: Questions from the Governing Board
- Undergo (and signpost all other Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards
- Support the academy in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and headteacher to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all academy staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole academy or college approach to online safety [with] a clear policy on the use of mobile technology"

Personal Development / RSHE Lead – Mr James Cooper

Key responsibilities:

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

Computing Lead – Mr Robert Howlett

Key responsibilities:

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

Subject / Faculty leaders

Key responsibilities:

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

Director of ICT Systems/other technical support roles – Mr Mark Beckett

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Note that KCSIE changes expect a great understanding of technology and its role in safeguarding when it comes to filtering and monitoring and in 2023/4 you will be required to support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the new DfE standards, protections for students in the home and remote-learning.
- Keep up to date with the academy'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 / LGfL nominated contact / RSHE lead to ensure that academy systems and networks reflect academy 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 academy's online security and technical procedures
- To report online-safety related issues that come to their attention in line with academy policy
- Manage the academy'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 academy technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with academy policy
- Work with the Headteacher to ensure the academy website meets statutory DfE requirements

Data Protection Officer (DPO) – Mr Richard Scott

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cybersecurity policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- Note that retention schedules for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records. 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 also monitored and audited

Volunteers and contractors (including tutor)

Key responsibilities:

- Read, understand, sign and adhere to our visitors information
- 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 academy and as part of remote teaching or any online communications
- A contractor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the academy, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Students

Key responsibilities:

- Read, understand, sign and adhere to the student acceptable use policy

Parents/carers

Key responsibilities:

- Read, sign and adhere to the academy's learning contract as completed at the beginning of the academic year when commencing in Year 7

External groups including parent associations – Parent Voice

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within academy
- Support the academy 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 academy staff, volunteers, governors, contractors, students or other parents/carers