The

MAST

Academy Trust

Policy	Online Safety Policy
Owner	Safeguarding Lead
Date approved	13th June 2023
Approver	Trust Board Standards and Effectiveness Committee

Current version	V2.0

Next review due	Summer 2024

Objective of Policy
Staying safe online

Version Control	
Version Number	Summary of amends from previous version
1.0	Development of the policy
2.0	Annual review

Sign off requirements	
Approvers	Position
Standards and Effectiveness Committee	Trust Board
Reviewers	Position
Natasha Greenough	CEO
Tim Wade	Trustee

Staying safe online

1.0 Acknowledgement

This policy is advised by '**YHGfL Guidance for Creating an esafety Policy'** written by Yorkshire and Humberside Grid for Learning. It has been adapted and updated by Kirklees Learning Service for use in Kirklees Schools including Independent schools and Academies.

2.0 Introduction

This Online Safety policy recognises the commitment of our schools in keeping staff and pupils safe online and acknowledges its part in the Trust's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe all of our school communities can benefit from the opportunities provided by the internet and other technologies used in everyday life. The Online Safety Policy supports this by identifying the risks and the steps we are taking to avoid them. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users (KCSIE 2022)
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm (KCSIE 2022)
- Commerce: online gambling, inappropriate advertising and phishing (KCSIE 2022)

This policy shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. We wish to ensure that all members of The Mast Academy Trust are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken. We aim to protect all pupils and our wider stakeholders in minimising the risk of misplaced or malicious allegations being made against adults who work with pupils.

Our expectations for responsible and appropriate conduct are set out in The MAST Academy Trust ICT and internet acceptable usage policy which we expect all staff and pupils to follow.
As part of our commitment to online safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets from loss or inappropriate use.

3.0 ***Policy Objectives;***

This policy applies to each school community within The Mast Academy Trust and includes the Senior Leadership Team (SLT), Local Governing Body (LGB), all staff employed directly or indirectly by the school, visitors and all pupils. Each Senior Leadership Team, led by the Executive Leadership Team will ensure that any relevant or new legislation that may impact upon the provision for online safety within school and reflected within this policy is understood and adhered to.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
The DFE Guidance on Searching, Screening and Confiscation (July 2022) gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any material that could be used to bully or harass others.

Each school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate online behaviour that take place out of school.

The person in school taking on the role of Online Safety lead is detailed in the school responsibilities document. The Governor with an overview of Safeguarding, including Online Safety matters is detailed in the school responsibilities document

4.0 Implementation of the policy

- Each school's Senior Leadership Team will ensure all members of school staff are aware of the contents of the Online Safety Policy and the use of any new technology within school.
- Staff, pupils and parents will be aware of the relevant Acceptable Use Policies/home school agreements (where appropriate and dependent on age of pupils) and will have ongoing access to this via the schools website.
- Any updates and/or amendments will be published and communicated to all stakeholders.
- Online safety will be taught as part of the curriculum in an age-appropriate way to all pupils.
- Online safety posters will be prominently displayed around the school.
- The Online Safety Policy will be made available to parents, carers and others via the school website or other online learning tools/apps used by individual schools.

5.0 Responsibilities of the School Community

We believe that online safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

5.1 The senior leadership team accepts the following responsibilities:

- The Headteacher will take ultimate responsibility for the online safety of the school community
- The nominated member of SLT will take day to day responsibility for online safety; provide staff updates as required. This is likely to be the SLT member with responsibility for Safeguarding in school.
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Develop and promote an online safety culture within the school community
- Ensure that all staff, pupils and other users agree to the ICT and Acceptable Use Policy and that new staff have this included as a part of their induction procedures.
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to online safety
- Receive and regularly review online safety incident logs; ensure that the correct procedures are followed should an online safety incident occur in school and review incidents to see if further action is required
- Online safety incidents are discussed with members of the DSL team as required and recorded via CPOMS in each school

5. 2 Responsibilities of the Online Safety Lead/Nominated member of SLT

- Promote an awareness and commitment to online safety throughout the school
- Be the first point of contact in school on all online safety matters (this may be delegated to members of the Pastoral teams in Middle School settings)
- Take day to day responsibility for online safety within the school
- Develop an understanding of current online safety issues, guidance and appropriate legislation through regular training
- Ensure that online safety education is embedded across the curriculum
- Ensure that online safety is promoted to parents and carers
- Ensure that any person who is not a member of school staff , who makes use of the school ICT equipment in any context, is made aware of the ICT and Acceptable Usage Policy
- With the support of the DSL, liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate
- Monitor and report on online safety issues to the Senior Leadership Team and the safeguarding/online safety governor as appropriate
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an online safety incident
- Ensure an online safety incident log is kept up to date (via cpoms, available in all schools)
- Ensure that good practice guides for online safety are displayed in classrooms and around the school.

5.3 Responsibilities of all Staff

- Read, understand and help promote the school's online safety policies and guidance
- Read, understand and adhere to the staff ICT and acceptable usage policy
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Ensure that all digital communication with pupils is on a professional level and only through school based systems, **NEVER** through personal email, text, mobile phone, social network or other online medium
- Embed online safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all online safety incidents which occur in the appropriate log and/or to their line manager
- Respect, and share with pupils the feelings, rights, values and intellectual property of others in their use of technology in school and at home.

5.4 Additional Responsibilities of Technical Staff

- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps, including filtering and monitoring, are in place to safeguard the security of the school IT system, sensitive data and information. Review these regularly to ensure they are up to date
- Ensure that provision exists for misuse detection and detection and prevention of malicious attack
- At the request of the Leadership Team conduct periodic checks on files, folders, email, internet use and other digital content to ensure that the Acceptable Use Policy is being followed
- Report any online safety related issues that come to their attention to the Online Safety Lead and/or Senior Leadership Team
- Ensure that suitable access arrangements are in place for any external users of the schools IT equipment
- Liaise with the Local Authority, internet providers and others as necessary on online safety issues
- Document all technical procedures and review them for accuracy at appropriate intervals
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

5.5 Responsibilities of Pupils

- Read, understand and adhere to the pupil AUP and follow all safe practice guidance (as appropriate to pupil age)
- Take responsibility for their own and each other's' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all online safety incidents to appropriate members of staff
- Discuss online safety issues with family and friends in an open and honest way
- To know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices, as appropriate to age phase.

5.6 Responsibilities of Parents and Carers

- Help and support the school in promoting online safety
- Read, understand and promote the pupil AUP with their children
- Discuss online safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Take full responsibility and monitor use of social media sites and be aware of the age restrictions in place for use of such platforms.
- Consult with the school if they have any concerns about their child's use of technology to take advice on how this can be managed.

- Understand the parental responsibility for pupils who use technology and social media outside of school and ensure this is managed appropriately.
- To agree to and sign the GDPR Consent Form which clearly sets out the use of photographic and video images of pupils.

5.7 Responsibilities of the Trust/LGB

- Read, understand, contribute to and promote the school's online safety policies and guidance as part of the school's overarching safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety awareness
- To have an overview of how the school IT infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data.

5. 8 Responsibilities of the Designated Safeguarding Lead

Be aware of and understand the risks to young people from online activities such as grooming for sexual exploitation, harmful sexualised behaviour/harassment, sexting, online bullying, radicalisation and others.

Attend regular training and updates on online safety issues. Stay up to date through use of online communities, social media and relevant websites/newsletters.

Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information.

Raise awareness of the particular issues which may arise for vulnerable pupils in the school's approach to online safety ensuring that staff know the correct child protection procedures to follow.

6.0 Teaching and Learning

We believe that the key to developing safe and responsible behaviours online for everyone within our school communities lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.
Our school's deliver a planned and progressive scheme of work to teach online safety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity. Online safety is taught in specific Computing and PSHE lessons and is also embedded across the curriculum, with pupils being given regular opportunities to apply their skills.
Our schools teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.
Our staff discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons.

7.0 How parents/carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.
To achieve this, we will offer opportunities for finding out more information through meetings, school newsletters and website and regular updates via our social media platforms.
We ask parents to be vigilant in their child's online activities and work with the school around any concerns raised.

7.1 Filtering

To be compliant with the Prevent Duty and Safeguarding Children in Education 2016, our school's will:

- Ensure that all reasonable precautions are taken to prevent access to unsuitable or illegal and extremist content. Web filtering of internet content is provided by Schools' Broadband; the provider is an IWF member and blocks access to illegal child abuse images and content. The provider filters the police assessed list of unlawful terrorist content produced on behalf of the home office. The school is satisfied that web filtering manages most inappropriate content including extremism, discrimination, substance abuse, pornography, piracy, copyright theft, self-harm and violence. It is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in pupils in monitoring their own internet activity, however, any incident where inappropriate materials have been accessed will be logged and fully investigated with the appropriate action taken.
- Inform all users about the action they should take if inappropriate material is accessed or discovered on a computer. Deliberate access of inappropriate or illegal material will be treated as a serious breach of the ICT and AUP and appropriate sanctions taken.
- Expect teachers to check websites they wish to use prior to lessons to assess the suitability of content.

7. 2 Monitoring

- School will use the findings of the annual Prevent risk assessment to put appropriate internet and network monitoring systems in place.
- Pupils are nearly always supervised by staff while using the internet as this reduces the risk of exposure to extremist, illegal or inappropriate material; direct supervision also enables school staff to take swift action should such material be accessed either accidentally or deliberately.
- Internet and network use is monitored regularly by the school technician to identify access to websites or internet searches which are a cause for concern.
- Impero network or classroom. Cloud monitoring software is used throughout school. This produces reports of inappropriate communications, searches and website access. Access to school systems

Each school decides which users should and should not have internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.
All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.
Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.
Remote access to school systems is covered by specific agreements and is never allowed to unauthorised third-party users.

7.3 Using the internet

We provide the internet to;

- Support teaching, learning and curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the LA, the examination boards and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.
All users of the school IT or electronic equipment will abide by the relevant ICT and Acceptable Use Policy at all times, whether working in a supervised activity or working independently,
Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school.

7.4 Using email

Email is regarded as an essential means of communication and the school provides all members of the school community (including pupils at middle school) with an email account for school based communication. Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. Email messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained. There are systems in place for storing relevant electronic communications which take place between school and parents.

Use of the school email system is monitored and checked.
It is the personal responsibility of the email account holder to keep their password secure.
As part of the curriculum pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.
School will set clear guidelines about when pupil-staff communication via email is acceptable and staff will set clear boundaries for pupils on the out-of-school times when emails may be answered.

Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email address. Responsible use of personal web mail accounts on school systems is permitted outside teaching hours.

7.5 Publishing content online

E.g. using the school website, learning platform, blogs, wikis, podcasts, social network sites

School website:

Each school maintains editorial responsibility for any school initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, e-mail and telephone number. Contact details for staff published are school provided.

Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the web site and school obtains permission from parents for the use of pupils' photographs. Group photographs do not have a name list attached.

7.6 Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multimedia and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

We ask all parents/carers to sign an agreement about taking and publishing photographs and video of their children (in publications and on websites) and this list is checked whenever an activity is being photographed or filmed.

We secure additional parental consent specifically for the publication of pupils' photographs in newspapers, which ensures that parents know they have given their consent for their child to be named in the newspaper and possibly on the website.

For their own protection staff, or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

7.7 Using mobile phones

Personal mobile devices belonging to pupils including mobile phones are permitted on school premises but must not be used within school hours or whilst pupils are on the school premises. Personal devices are brought onto school premises by pupils at their own risk and each school will determine their own policy for storage of mobile phones during the school day. The school does not accept liability for loss or damage of personal devices. Each school will have their own guidelines and rules on the safe keeping of mobile phones during the school day.

Where required for safety reasons in off-site activities, a school mobile phone may be provided for staff for contact with pupils, parents or the school. Staff will never use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent. In an emergency, where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures

or video is forbidden. Publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request.
The sending or forwarding of text messages, emails or other online communication deliberately targeting a person with the intention of causing them distress is online bullying; this will be considered a disciplinary matter.

7.8 Using wearable technology

Wearable technology includes electronic fitness trackers and internet enabled 'smart' watches. Wearable technology is permitted on school premises but must not be used within school hours. Personal devices are brought onto school premises by pupils at their own risk. The school does not accept liability for loss or damage of personal devices. Wearable technology is not to be worn during tests or examinations.

7.9 Using mobile devices

We recognise that the multimedia and communication facilities provided by mobile devices (e.g. iPad, iPod, tablet, netbook, Smart phones) can provide beneficial opportunities for pupils. However, their use in lesson time will be with permission from the teacher and within clearly defined boundaries.
Pupils are taught to use them responsibly.

7.10 Using other technologies

As a school we will keep abreast of new technologies and evaluate both the benefits for learning and teaching and also the risks from an online safety point of view.
The Trust will regularly review the online safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.
Staff or pupils using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to the same standards of behaviour to those outlined in this document.

7. 11 Responding to online safety incidents

All serious online safety incidents are recorded on CPOMS which is regularly reviewed by the DSL team.
Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.
In situations where a member of staff is made aware of a serious online safety incident concerning pupils or staff, they will inform the Online Safety Lead/DSL who will then respond in the most appropriate manner.
Instances of **online bullying** will be taken very seriously by the school and dealt with using the school's anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.
Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's Online Safety Lead and technical support and appropriate advice sought and action taken to minimise the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy, then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.
School reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

8.0 Dealing with complaints and breaches of conduct by pupils:

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to a senior member of staff
- Parents and the pupil will work in partnership with staff to resolve any issues arising
- Restorative practice will be used to support the victims
- There may be occasions when the police must be contacted and/or concerns shared with Local Authority Children's services (in line with Safeguarding policy and KCSIE 2022).

8.1 The following activities constitute behaviour which we would always consider unacceptable (and possible illegal):

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- continuing to send or post material regarded as harassment or of a bullying nature after being warned

Staff using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites).

8.2 The following activities are likely to result in disciplinary action:

- any online activity by a member of the school community which is likely to adversely impact on the reputation of the school
- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute
- attempting to circumvent school filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- Revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission.
- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarizing of online content)
- Transferring sensitive data insecurely or infringing the conditions of the Data Protection Act 1998.

8.3 The following activities would normally be unacceptable; in some circumstances they may be allowed e.g. as part of planned curriculum activity or by a system administrator to problem solve

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time

- accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
- sharing a username and password with others or allowing another person to log in using your account
- accessing school ICT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

Any questions relating to the online safety policy should be directed to the nominated member of SLT in the individual school concerned details of which can be found in the school responsibilities document.