MOSAIC SCHOOLS LEARNING TRUST

MOSAIC
SCHOOLS LEARNING TRUST

Online Safety Policy

All schools in Mosaic Schools Learning Trust are committed to safeguarding and promoting the welfare of children and young people and expect all staff and volunteers to share this commitment.

Unicorn
PRIMARY SCHOOL

Document Detail	
Category	Online Safety
Authorised By	Rebecca Strong
Status	
Approved By	
Date of Review:	March 2026
Date of Next Review	October 2026
Version	5

SUMMARY OF CHANGES

Date	Change
28/11/24	Overhaul of current online safety policy by RS
12/03/2026	• Changes made to reflect KCSIE 2025 and any recent guidance • Changes made to include new service provider – Eduthing • Changes made to align with new Responsible Use of Artificial Intelligence Policy Made by RS

Contents

1. Introduction

What is Online Safety?

It can be called E Safety (or e-safety), Online Safety or Internet Safety, but it all means the same thing. It's about risk; it's about being aware of the possible threats that online activity can bring, and how to deal with them.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

This policy explains how we aim to protect and support children when they are using technology to support their education, within school and within the wider community.

The Policy applies to all members of the school community (including staff, students/ pupils, volunteers, parents/carers, visitors, community users) who have access to, and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers 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 cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

2. Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

In addition, it reflects the Education Act 2011, which has given teachers stronger powers with regard to the searching of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published behaviour policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policy and will, where known, inform parents/carers of incidents of inappropriate online behaviour.

The policy also takes into account the National Curriculum Computing programmes of study, Relationships, Health and Sex Education and the Computing curriculum.

3. Roles and Responsibilities

3.1 The Governing Board

The governing board is responsible for:

- The approval of the Online Safety policy and for reviewing the effectiveness of the policy.
- Appointment of online safety Governor (can be the safeguarding governor), this role will include:
    - regular meetings with the Online Safety Lead/DSL
    - regular monitoring of online safety incident logs
    - regular monitoring of filtering logs
    - reporting to Local Governing Body meetings
- Checking that provision outlined in the Online Safety Policy e.g., online safety education provision and staff training is taking place as intended
- Ensuring that the filtering and monitoring provision is reviewed and recorded, in line with this policy
- Holding the Headteacher to account for the implementation of this policy.

3:2 The Network Manager – Eduthing

Responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets the required online safety technical requirements.
- Users may only access the networks and devices through properly enforced password protection, in which passwords are regularly changed;
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- The use of the network/internet is regularly monitored in order that any misuse/attempted misuse can be reported to the Head teacher and DSL for investigation/action;
- Monitoring software/systems are implemented and updated as agreed in school policies.
- Report filtering breaches

3.3 The Headteacher and The Senior Leadership Team

The Headteacher along with Senior leaders are responsible for:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the DSL and Online Safety Lead

- The Headteacher/ Senior Leadership Team must be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher/ Senior Leadership Team are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher/ Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role/s.
- The Senior Leadership Team will receive regular monitoring reports

It is noted that the Whistleblowing Policy may be relevant in some cases.

3:4 The Designated Safeguarding Lead

• Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
• Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
• Provides training and advice for staff.
• Liaises with Bromley Safeguarding Board.
• Liaises with technical staff and IT support suppliers.
• Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, meets regularly with Safeguarding/Online Safety Governor to discuss current issues, review incident logs and filtering/monitoring control logs.
• Attends relevant meeting/committee of Governors.
• Reports regularly to Senior Leadership Team.

The DSL should be trained in online safety issues and be aware of the potential for serious child protection/ safeguarding issues to arise from:

- sharing of personal data
- access to illegal/ inappropriate materials;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming; and
- cyber-bullying

3:5 Computing Subject Lead/s, teaching and support staff

Responsible for ensuring that:

- Staff will act as good role models in their use of digital technologies the internet and mobile devices.
- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices;

- they have received appropriate safeguarding and child protection training (aligned with KCSIE guidance), including online safety. As part of their training, they should understand their roles and responsibilities with filtering and monitoring.
- they have read, understood and signed the Staff Acceptable Use Agreement (AUA);
- they report any suspected misuse or problem to the Headteacher / Senior Leadership Team; for investigation/action/sanction;
- all digital communications with pupils/parents/carers must be on a professional level and only carried out using official school systems;
- online safety issues are embedded in all aspects of the curriculum and other activities;
- pupils understand and follow the online safety and acceptable use policies;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices; and
- in lessons where internet use is pre-planned pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

3:6 Parents and Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

The school will take every opportunity to help parents understand these issues through means such as: newsletters, letters, the school website and signposting parents to recommended external websites and webinars. The school will share information about national/local online safety campaigns/literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice.

Parents will read Pupil Acceptable Use Policy in KS1 and KS2 (see appendix)

3:7 Community users

Community Users who access school systems/website as part of the wider school provision will be expected to adhere to school policy.

3:8 Pupils

Pupils must understand that they:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy;
- KS1 and KS2 pupils will read and sign Pupil Acceptable Use Policy

- need to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand school rules on the use of mobile devices;
- know and understand policies on the taking/use of images and on cyber-bullying; and
- know the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety Policy covers their actions out of school, if related to their membership of the school.

3.9 Data Protection Officer

The **DPO is embedded in the below:**

- filtering & monitoring decisions
- cyber security governance
- AI-related DPIAs

4 School Policy and Procedures

4:1 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4: 2 GDPR (2018)

When using data (including images or evidence from online activities) all Unicorn staff will be aware of our, Data Protection Policy and Privacy Notice Policies

4:3 Security and Management of Information Systems

The school takes appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- The appropriate use of user logins and passwords to access the school network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

4:4 Photographs and Videos

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud-based services (e.g., See Saw, Arbor or in the Media Share Drive).

As part of our school activities, we may take photographs and record images of individuals within our Trust.

See our Safeguarding and Data Protection Policy for more information on our use of photographs and videos.

Parents are asked to provide consent for the situations in which the school may use photographs of their child e.g. in school, on the school website, in outside publications. This is done via their account on the school IMS Arbor and can be updated if there is a change of preference.

4:5 Use of Personal Mobile Devices

- Staff, Parents and Careers and pupils will not use technology in school to view material that is illegal, inappropriate or likely to be deemed offensive. This includes, but is not limited to, sending obscene emails, gambling and viewing pornography or other inappropriate content.
- The school allows staff, including temporary and peripatetic staff to use personal mobile phones and devices but never in the presence of pupils.
- Visitors will be made aware that they should not use mobile phones whilst on site, and that under no circumstances should they take photographs
- Under no circumstance does the school allow a member of staff to contact a pupil using their personal device.
- If a parent/carer needs to be contacted, staff should use the school landline, or in the event of needing to contact a parent on a personal device (e.g., school trip) the caller's number must be withheld.
- Year 5 and 6 pupils are allowed to bring personal mobile phones to school, but only if they are walking home alone. The teacher must be made aware of this and pupils' phones are to be kept securely in the office or out of reach in their classroom cupboard during the school day. Phones must be switch off on arrival in school.
- Under no circumstance should pupils use their personal mobile devices/phones to take images of any other pupil
- The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Other than for training/teaching/performance events where consent has been obtained, staff, parents/carers and pupils will not make audio or video recordings.
- Parents/carers or staff will not make recordings of meetings. The covert recording of colleagues will be considered an act of misconduct.

See our Mosaic Staff Code of Conduct Policy for more information

4:6 Communication and Social Media

Staff

School staff's social media profiles should not be available to pupils. If they have a personal profile on social media sites, we would recommend that staff should not use their full name, as pupils may be able to find them. Staff should consider using a first and middle name or similar instead, and set public profiles to private.

Staff should not attempt to contact pupils or their parents via social media, or any other means outside school, in order to develop any sort of relationship. They will not make any efforts to find pupils' or parents' social media profiles.

Where there is an existing relationship between an adult working within the school and a child attending the school, the social media sites used by staff members will be restricted to private accounts that do not have any link to other pupils attending the school. There should be no social media contact between any members of staff and a pupil that is not their direct family/friends.

Staff will ensure that they do not post any images online that identify children who are pupils at the school other than on school websites and with the appropriate consent.

Staff should understand the expectations set out in their school's Trust's ICT Acceptable Use Policy and Staff Code of Conduct Policy.

Parents, carers and pupils

Parents, careers and pupils should not attempt to contact staff via social media, or any other means outside school, in order to develop any sort of relationship.

Where there is a relationship between an adult working within the school and a parent, carer or child attending the school, the social media sites used by staff members will be restricted to private accounts that do not have any link to other pupils attending the school. There should be no social media contact between any members of staff and a pupil that is not their direct family/friends.

4: 7 Use of AI

Artificial Intelligence (AI) technology is already widely used in both commercial and everyday applications, and its influence is anticipated to grow exponentially, impacting almost all industries and job sectors including education. Generative AI refers to technology that can be used to create new content based on large volumes of data that models have been trained on from a variety of works and other sources. Generative AI is a rapidly evolving and increasingly freely available technology generating writing, audio, codes, images and video simulations. Whilst this offers opportunities for schools and their pupils, it also increases risk.

AI is an integral part of the modern world and offers numerous opportunities for enhancing teaching, learning, and administrative processes. This policy establishes guidelines for the responsible and effective use of AI within our School.

By embracing AI technology, we aim to:

- Enhance academic outcomes and educational experiences for pupils

• Support teachers in managing their workload more efficiently and effectively

• Educate staff and pupils about safe, responsible and ethical AI use

• Incorporate AI as a teaching and learning tool to develop staff and pupils' AI literacy and skills

• Prepare staff and pupils for a future in which AI technology will be an integral part

• Promote equity in education by using AI to address learning gaps and provide personalised support

• Improve and streamline school operations to minimise cost and maximise efficiency.

All users of AI will comply with applicable laws, regulations, policies and guidelines governing Keeping Children Safe in Education, intellectual property, copyright, data protection and other relevant areas. There will be no unauthorised use of copyrighted material or creation of content that infringes on the intellectual property of others. We will prioritise the safeguarding of our pupils and their online safety and will not knowingly use any AI technology that puts their safety or privacy at risk. Staff will not allow or cause intellectual property, including pupils' work, to be used to train Generative AI models without appropriate consent or exemption to copyright.

We recognise that technology is rapidly evolving and are committed to remaining at the forefront of developments, adapting our ways of working as necessary. We recognise the leadership in the education sector provided by the Department of Education and the guidance set out in their policy paper on Generative Artificial Intelligence in Education. This AI policy has been informed by that guidance. As guidance and technology changes, the policy therefore will need to remain under regular review. This policy will be reviewed annually.

We will be transparent and accountable about the use of AI technology so that stakeholders, including staff, pupils, parents and other partners understand where and how AI is used and who is responsible. Any stakeholder feedback or questions about the use of AI will be considered and responded to appropriately.

We will treat any use of AI to bully pupils in line with our Anti-Bullying and Behaviour and Relationships Policies.

See our Mosaic policy; 'Responsible Use of Artificial Intelligence' for more information

4: 8 Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or

inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Unicorn will review annually filtering and monitoring using the **Plan Technology for Your School** self-assessment tool, self-assessment tool as outlined in KSCIE 2025. This will be used to assess against the filtering and monitoring standards and recommendations on how to meet them.

- review filtering/monitoring annually
- evidence actions taken

Decision Making

- Unicorn Primary School has ensured that it has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The Governors and Senior Leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The schools' decisions regarding filtering and monitoring have been informed by a risk assessment, taking into account our school's specific needs and circumstances.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.
- In lessons where internet use is pre-planned, it is best practice that pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.

Filtering

The school uses the London Grid for Learning (LGFL) filtering system, which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff and a member of the senior leadership team can temporarily remove those blocked sites from the filtered list for the period of study. Any request to do so, will be auditable, with clear reasons for the need.

Monitoring

The school will appropriately monitor internet use on all school owned or provided internet enabled devices. All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

5: Inappropriate Use

5: 1 Records, Monitoring and Review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

5:2 Filtering and Monitoring Breaches

The school has a clear procedure for reporting breaches:

- If pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediate to a member of staff.
- The member of staff will report to the Head Teacher and/or technical staff.
- The member of staff will record the concern on SmoothWall, including the URL of the site if possible
- The breach will be escalated as appropriate.
- Parents/carers will be informed of the breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies.

5: 3 Misuse of Technology

There may be occasions in school when either a pupil or an adult receives or is aware of an offensive, abusive or inappropriate message or intentionally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff.

Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, one of the designated safeguarding leads will refer details to Bromley social care and/or the police.

Should a child be found to intentionally misuse the online facilities whilst at school, the following consequences should occur:

- Where a child is found to be misusing the internet by not following the Acceptable Use Agreement a phone call to parents will be made explaining the reason for suspending the child's use for a particular lesson or activity. Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time.
- Parents will be contacted outlining any breach where a child is deemed to have misused technology against another child or adult.

Children will be taught and encouraged to consider the implications for misusing the internet/school technology resources e.g. understanding the potential legal implications.

5: 4 Child on Child abuse Online Bulling/Cyberbullying

Online Bullying/Cyberbullying is the use of technology (social networking, messaging, text messages, e-mail, chat rooms etc.) to ridicule, harass, threaten or intimidate someone. There are other forms of abuse that may occur between peers and this list is not exhaustive. See appendix 1 for the full list of unsuitable/inappropriate activities

Cyberbullying, along with all other forms of bullying, will not be tolerated and will be dealt with in line with the schools' Anti-bullying Policy.

5:5 Online Child Sexual Abuse and Exploitation

If school staff are made aware of incident involving online sexual abuse of a child, they will:

• Act in accordance with the school's Safeguarding and Child Protection policy and procedures.
• Immediately notify the Designated Safeguarding Leads.
• Store any devices involved securely.

The DSL will:

• Immediately inform the police via 101 (or 999 if a child is at immediate risk)
• Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
• Inform parents/carers about the incident and how it is being managed.
• Make a referral (if required/ appropriate).
• Provide the necessary safeguards and support for pupils, such as, offering pastoral support.

5: 6 Online Radicalisation and Extremism

• The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
• If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Head Teacher will be informed immediately, and action will be taken in line with the Safeguarding and Child Protection Policy with specific regard to 'Prevent' actions/protocols.
• If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the Safeguarding and Child Protection policy with specific regard to 'Prevent' actions/protocols.

5: 7 Concerns about Pupils Welfare

• The Head Teacher will be informed of any online safety incidents involving safeguarding or child protection concerns
• The Head Teacher will ensure that online safety concerns are escalated and reported to relevant agencies in line with relevant thresholds and procedures.
• The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

6 Teaching and Learning

6: 1 Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety will be a focus in all areas of the curriculum and staff will reinforce online safety messages across the curriculum. The online safety curriculum will be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Online safety will be provided as part of Computing/PHSE/other curriculums and will be regularly revisited.
- High profile events/campaigns e.g., Safer Internet Day will have a bespoke curriculum and a highlighted focus within the school day
- Outside agencies will be employed to support the curriculum e.g. The Life Bus and BRECK Foundation

Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities:

- Children will be taught where to go for help and the important role of the trusted/appropriate adult.
- Children will be taught how to report content and activity that worries them
- Children will be taught how to protect their privacy/identity online
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

For a detailed overview of the curriculum please see Appendix 4: Curriculum Overview

6:2 Education – Parents/Carers

Parents and carers play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Keeping Children Safe in Education states that schools should use communications with parents and carers to reinforce the importance of children being safe online.

The school seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, bespoke website page/s
- Parent focused webinars provided by external providers e.g., Knowsley Trust
- Parents/carers sessions e.g., an online safety evening or information provided at parents' evenings
- High profile events/campaigns e.g., Safer Internet Day
- Reference to the relevant websites/publications

6:3 Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

Training and support for all staff will be provided as follows:

- Online safety will be part of annual safeguarding and child protection training.
- Specific online safety training sessions
- Staff newsletters provided by Knowsley Trust and termly webinars covering subject including; new and emerging threats and policy amendments
- The DSL/Online Safety Lead will receive regular updates through attendance at external training events (e.g., from LGfL/Bromley DSLs forum/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety Policy and its updates will be presented to and discussed by staff in staff/ team meetings/INSET days.
- The Online Safety Lead/Computing Lead will provide advice/guidance/training to individuals as required.

6:4 Training – Governors

Governors receive relevant online safety training as part of annual safeguarding and child protection training. Those who hold link roles involved in technology/online safety/health and safety/child protection may be signposted towards further training and all governors will have an open invitation to attend staff training sessions.

Governors will have access to:

- newsletters provided by Knowsley Trust and termly webinars covering threats and policy

- Training Sessions provided by National College and GovHub
- Training provided by the Local Authority/National Governors Association/or other relevant organisation (eg LGfL).

7 Links with Other Policies

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

It is linked to the following other school policies and documents:

- Anti-Bullying Policy
- Behaviour and Relationships Policy
- Data Retention Policy
- Equality Act 2010
- GDPR Policy
- Health and Safety
- Home–School Agreement
- ICT Acceptable Use Policy
- Mosaic Staff Code of Conduct Policy
- Privacy Notice Policies
- Responsible Use of Artificial Intelligence Policy
- Safeguarding Policy
- Whistleblowing Policy

8: Monitoring and Review

This policy will be reviewed annually. We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

Appendix 1: Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems:

Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008.
- Any other form of pornography
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986.
- Promotion of any kind of discrimination.
- Threatening behaviour, including promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Users should not:

- Use school systems to run a private business.
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy.
- Infringe copyright.
- Reveal or publicise confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords).
- Create or propagate computer viruses or other harmful files.

Users should refrain from using school systems and resources for personal recreational activities for example:

- Online gambling.
- Online shopping/commerce.
- Use of social media.
- Use of messaging apps.
- Pupils unsupervised use of video broadcasting e.g. Youtube

Appendix 2: Pupil Acceptable Use Policy; KS1

KS1 Computing Rules

S 	I will only use an iPad or computer with the permission of a trusted adult.
A 	I will only use kind words online.
F 	I will only communicate online with people I know in real life, unless I have a trusted adult with me.
E 	If I see something I don't like on a screen, I will always tell an adult.
T 	I will always keep my passwords to myself.
Y 	I will look after all IT equipment, including iPads and computers.
I have read these rules, and I will do my very best to follow them inside and outside of school. My Name:	

Appendix 3: Pupil Acceptable Use Policy; KS2

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and are part of the Unicorn Primary School Home-School Agreement.

I understand that there may be consequences if I do not follow these rules either at school, outside of school, and online.

Conduct:

• I will only use the school's iPads/computers for educational use.

• I will only edit or delete my own files/online accounts and not change or log into other people's files/online accounts without their permission.

• I will keep my logins and passwords to myself.

Contact:

• The messages I send, or information I upload, will always be polite and sensible.

• I will only message people I know, or a responsible adult has approved.

• I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.

• I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family, my school or my friends, unless a trusted adult has given permission.

Content:

• If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult, and try to take a screenshot as evidence.

• I am aware that some websites and social networks have age restrictions and I should respect this, as well as understand that these restrictions are in place to protect me.

• I will not attempt to visit Internet sites that I know to be banned by the school, or that would be inappropriate for home use.

• I will not open an attachment, or download a file, unless I know and trust the person who has sent it. I have read and understand these rules and agree to follow them at all times, and be a good Digital Citizen.

Signed (pupil): Date:

Signed (parent): Date:

Appendix 4: Online Safety Curriculum Progression Map

Computing Level Expected at the End Of EYFS			
Reception	Personal, Social and Emotional Development		• Show resilience and perseverance in the face of a challenge. • Know and talk about the different factors that support their overall healthand wellbeing: -sensible amounts of 'screen time'.
ELG	Personal, Social and Emotional Development	Managing Self	• Be confident to try new activities and show independence, resilience andperseverance in the face of challenge. • Explain the reasons for rules, know right from wrong and try to behave accordingly.

Year Group	National Curriculum Objectives	Skills/Knowledge	Coverage against
EYFS	Children recognise that a range of technology is used in places such as homes and schools. They select and use technology for particular purposes.	1. To describe what personal information is. 2. To identify examples of personal information. 3. To describe the adults I can trust and know I can always ask for help. 4. To describe ways that some people can be unkind online. 5. To recognise when to say 'no' if something may upset or embarrass you in real life or online. 6. To identify some ways technology is used at home and in school. **Education for a connected world** A= Self imagine and identity B = online relationships C= online reputation D= online bullying E= managing online information F = heath, well-being and lifestyle G= Privacy and Security H= Copyright and ownership	• **Spring 1:** PSHE: Keeping safe online: 3, 4, 5, 6, A, B, C, G • **Spring 1:** Internet Safety Day: February 6th 2024: Inspiring Change: Making a difference, managing influence and navigating change online: 3,4,5,6, A, B, C, D, F, H • **Spring 2:** Computing: e–safety – tbc: personal information. 1,2,3 E, G,

Year Group	National Curriculum Objectives	Skills/Knowledge	Coverage against:
Year 1	***Across Year 1 and Year 2*** - Recognise common uses of information technology beyond school - Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about material on the internet or other online technologies	1. To recognise more detailed examples of personal information. 2. To explain how passwords can be used to protect my information. 3. To give examples on how to behave considerately online in ways that do not upset others. 4. To identify what to do if they see disturbing content online at home or at school 5. To understand that information on the internet can be seen by others. **Education for a connected world** A= Self imagine and identity B = online relationships C= online reputation D= online bullying E= managing online information F = heath, well-being and lifestyle G= Privacy and Security H=Copyright and ownership	• **Autumn 1:** Computing: e-safety- I understand what persona; information I need to keep safe: 1,2,4,5, B, E, G • **Spring 1**: PSHE: Sharing pictures: 1, 3, 4, 5, A, B, C, E, G • **Spring 1:** Internet Safety Day: February 6th 2024: Inspiring Change: Making a difference, managing influence and navigating change online: 3,4,5,6, A, B, C, D, F, H Holistic coverage via PSHE curriculum: • **Summer 1:** Pass on the praise! B, H • **Autumn 1**: Good friends, B, • **Spring 1:** Who can help? (1) D

Year 2		1. To explain what personal information is and develop awareness of why it is special and should not be shared. 2. To give examples of online bullying and discuss how it might make someone feel. 3. To explain how other people's identity online can be different to their identity in real life. 4. To explain what to do if they have concerns about content or contact online. 5. To identify ways they can use the Internet to communicate with family and friends. **Education for a connected world** A= Self imagine and identity B = online relationships C= online reputation D= online bullying E= managing online information F = heath, well-being and lifestyle G= Privacy and Security H=Copyright and ownership	• **Autumn 1:** Understand why it's important to stay safe online: 1, 2, 3, 4, 5, B, E, G, • **Spring 1:** PSHE: Playing games: 1, 3, 4,A, B, E, G, • **Spring 1:** PSHE: Should I tell: 3, 4, b, C, D • **Spring 1:** Internet Safety Day: February 6th 2024: Inspiring Change: Making a difference, managing influence and navigating change online: 3,4,5,6, A, B, C, D, F, H **Holistic coverage via PSHE curriculum:** • **Autumn 1:** PSHE/L Being a good friend: 2, B • **Autumn 2:** PSHE: Solve the Problem: 2, E • **Autumn 2:** PSHE: How do we make others feel? 1,2, B, • **Spring 1:** PSHE: What should Harold say? 4, D, • **Spring 2**: PSHE: Feeling safe, 4, B, F, • **Summer 2:** PSHE: Respecting Privacy: 1, B, G, H • **Summer 2:** PSHE: My body, your body: 1, A

Year 3	***Across Year 3, Year 4, Year 5 and Year 6*** - Understand computer networks including the internet; how they can provide multiple services, such as the world-wide web; and the opportunities they offer for communication and collaboration - Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content - Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact	1. To identify who they can trust and share their personal information with online. 2. To identify how to report concerns and inappropriate behaviour in school. 3. To describe rules about how to behave online and how to follow them. 4. To decide whether a web page is relevant and reliable for a given purpose or question. 5. To explain what it meant by the term 'identity'. 6. To identify the risks about my identity online (e.g. online gaming, social media) and know how to protect themselves (e.g. using an avatar and a nickname). **Education for a connected world** A= Self imagine and identity B = online relationships C= online reputation D= online bullying E= managing online information F = heath, well-being and lifestyle G= Privacy and Security H=Copyright and ownership	• **Autumn 1**: e-safety: What is meant by cyberbullying: 2, 3, 6, B, D, F (also taught, in Autumn 2, SMART recap and Personal info and reliable websites) 1, 2, 4, B, E, G, H • **Autumn 1:** PSHE: As a rule, 2, 3, B • **Autumn 2:** PSHE; Zeb, 1, 2, 3, B, D, • **Spring 1:** Super Searcher; 1, 4, 5, 6, C, E, H • **Spring 1:** Internet Safety Day: February 6th 2024: Inspiring Change: Making a difference, managing influence and navigating change online: 3,4,5,6, A, B, C, D, F, H • **Summer 2:** PSHE; None of your business, 1, 2, 4, 5, 6, A, B, C, D, E. G **Holistic coverage via PSHE curriculum** • **Autumn 2**: Let's celebrate our differences; 2, 3, B, D • **Spring 1,** PSHE; Raisin Challenge, 6, • **Summer 1:** I am fantastic, 2, 3, A • **Summer 1**: Relationship Tree, 1, 4, 5, 6, D, *Note: copyright and ownership:* Cdo learn about respectful behaviours, both online and offline holistically through the SCARF curriculum. Respecting the rights of others is explored in the PSHE Rights and Respect unit, across KS2

Year 4		1. To demonstrate that they can act responsibly when using internet. 2. To identify and explain the differences between acceptable and unacceptable behaviours when using digital technology. 3. To know who to talk to about concerns and inappropriate behaviour at home or in school. 4. To understand that others online can pretend to be me or others, including my friends. 5. To describe the right decisions about how I interact with others and how others perceive me. **Education for a connected world** A= Self imagine and identity B = online relationships C= online reputation D= online bullying E= managing online information F = heath, well-being and lifestyle G= Privacy and Security H=Copyright and ownership	• **Autumn 1:** e-safety objectives: o What is plagiarism o Define cyberbullying (also taught, in Autumn 2, Online dangers AND acceptable vs unacceptable behaviours) 1, 2, 3, 4, 5, A, B, C, D, E, G, H • **Autumn 1:** PSHE: Under pressure. 1, 2, 3, 5, A, F • **Autumn 2:** PSHE; That is such a stereotype! 2, 4, 5, C • **Spring 1:** Internet Safety Day: February 6th 2024: Inspiring Change: Making a difference, managing influence and navigating change online: 3,4,5,6, A, B, C, D, F, H • **Spring 1:** PSHE: Danger, risk or hazard? 2, 3, 4, B, G, H • **Spring 1:PSHE**: Picture wise. 1, 2, 3, 4, 5. C, E, H • **Spring 1:** PSHE: Traffic lights: 2, 3, 4, C, E, • **Spring 2**: PSHE: In the news! 2, 3, A, E, • **Summer 1:** PSHE: SCARF hotel: links to self-image and identify outlined in a connected world, F, A **Holistic coverage via PSHE curriculum:** • **Autumn 1**: PSHE: Ok or not ok? (part 2). 2, A, B, D, G • **Spring 2**: PSHE: How do we make a difference? 5, B, C, D, E, • **Autumn 2**: PSHE: Can you sort it? 2, 3, B, D, • **Spring 1:** PSHE: How dare you. 1, 5, D, • **Autumn 1**: PSHE: An email from Harold! 1, F • **Spring 1:** PSHE: Keeping ourselves safe. 2, 3,4,C, E,
Year 5		1. To demonstrate that they can act responsibly when using the internet. 2. To discuss the consequences of particular behaviours when using digital technology. 3. To know how to report concerns and inappropriate behaviour in a range of contexts. 4. To demonstrate responsible choices about my online identity, depending on context. 5. To decide whether digital content is reliable and unbiased. **Education for a connected world** A= Self imagine and identity B = online relationships C= online reputation D= online bullying E= managing online information F = heath, well-being and lifestyle G= Privacy and Security H=Copyright and ownership	• **Autumn 1**: e-safety: To understand how to use technology safely, respectfully and responsibly. Including, acceptable vs unacceptable behaviours, passwords, SPAM, sites to cite. 1, 2,3, 4, A, B, C, E, G • **Autumn 1:** PSHE: Communication. 1, 2, 3, B, C, D, E • **Autumn 2:** PSHE: Is it true? 4, 5, B, C, D, E, • **Autumn 2:** Anti bullying week: Introduction to Cyberbullying and Is It Funny or Is It Hate? 1, 2, 3, 4, A, B, C, D, E, F • **Spring 1:** PSHE: Spot bullying. 1, 2, 4, A, B, C, D, E, G • **Spring 1:** PSHE: Play, like, share 1, 2, 3, A, B, C, D, E, G • **Spring 1:** Internet Safety Day: February 6th 2024: Inspiring Change: Making a difference, managing influence and navigating change online: 3,4,5,6, A, B, C, D, F, H • **Spring 2**: PSHE: What's the story? 4, 5, F • **Spring 2**: PSHE: Fact or opinion? 3, 4, 5, B, C, D, E, H • **Summer 1:** PSHE: Star Qualities 5, A

Year 6		1. To demonstrate that they can act responsibly when using the internet. 2. To discuss the consequences of particular behaviours when using digital technology. 3. To explain when to block abusive users. 4. To know how to report concerns, online bullying and inappropriate behaviour in a range of contexts. 5. To explain how identity can be copied, modified or altered. 6. To decide whether digital content is reliable and unbiased. **Education for a connected world** A= Self imagine and identity B = online relationships C= online reputation D= online bullying E= managing online information F = heath, well-being and lifestyle G= Privacy and Security H=Copyright and ownership	• **Autumn 1**: e-safety: To explain how identify can be copied, modified or altered, A, B, E, G • **Autumn 2:** Boys will be boys? Challenging gender stereotypes. 1, 5, 6, B, F, D, H • **Autumn 2:** Anti bullying week: Introduction to Cyberbullying and Is It Funny or Is It Hate? 1, 2, 3, 4, A, B, C, D, E, F • **Spring 1**: Think before you click! 1, 2, 3, 4, 6, B, C, D, E, H • **Spring 1**: **It's** a puzzle. 2, 3, 4, 5, B, C, D, E, • **Spring 1:** Two sides to every story 5, 6, F, C, D, F • **Spring 1:** PSHE: To share or not to share? 1, 2, 4, A, C, E, G, • **Spring 1:** Internet Safety Day: February 6th 2024: Inspiring Change: Making a difference, managing influence and navigating change online: 3,4,5,6, A, B, C, D, F, H • **Spring 2**: Fakebook friends. 1, 2, 3, 4, 5, A, G • **Summer 1:** What's the risk? (2) 2, 4, 5, A, C, G • **Summer 2**: I look great! 5, 6, A, D, H • **Summer 2**: Media manipulation 2, 5, 6, A, H • **Summer 2:** Pressure online, 1, 2, 3, 4, A, C, E, G **Holistic coverage via PSHE curriculum:** • **Spring 1:** PSHE: Joe's story (part 2), A, • **Autumn 2:** PSHE: We have more in common than not. 1, B, D, • **Spring 1**: PSHE: Rat Park • **Summer 1:** PSHE: Five Ways to Wellbeing project, F • **Autumn 1:** PSHE: Advertising friendships! 4, F • **Summer 2**: Helpful or unhelpful? Managing change. 1, 2, 3, F • **Summer 2**: It's a puzzle: B, C, D, E