Urbis Academy Trust
Esse Optimus Qui Possum

Mayville Primary School

Online Learning Policy

2021-2022

Approved by:	Audit and Resources Committee	**Date:** 6 October 2021
Last reviewed on:	September 2021	
Next review due by:	September 2022	

1. AIMS

1.1 Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees
- Deliver an effective approach to online safety, which empowers us to protect and educate
- the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. LEGISLATION AND GUIDANCE

2.1 This policy is based on the Department for Education's (DfE) Statutory Safeguarding Guidance, Keeping Children Safe in Education 2021, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff
- Searching, screening and confiscation.

2.2 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 to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

2.3 This policy complies with our funding agreement and articles of association.

3. ROLES AND RESPONSIBILITIES

3.1 The Governing Board

3.1.1 The trustees have overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

3.1.2 The trustees will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

3.1.3 All trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3).

3.2 The Headteacher

3.2.1 The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

3.3.1 Details of the school's DSL deputies are set out in our child protection and safeguarding policy, as well relevant job descriptions.

3.3.2 The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board.
- This list is not intended to be exhaustive.

3.4 The ICT Manager

3.4.1 The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keeping pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- Conducting a full security check and monitoring the school's ICT. Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

3.5.1 All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- This list is not intended to be exhaustive.

3.6 Parents

3.6.1 Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

3.6.2 Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.7 Visitors and Members of the Community

3.7.1 Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

4.1 Pupils will be taught about online safety as part of the curriculum:

Following guidance from the National Curriculum Computing Programmes of Study.

4.2 In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

4.3 Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact.

4.4 By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships and face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

4.5 The safe use of social media and the internet will also be covered in other subjects where relevant.

4.6 The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. EDUCATING PARENTS ABOUT ONLINE SAFETY

5.1 The school will raise parents' awareness of internet safety via letters, the school website and the weekly Newsletter. This policy will also be shared with parents. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

5.2 Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. CYBER-BULLYING

6.1 Definition

6.1.1 Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy).

6.2 Preventing and Addressing Cyber-Bullying

6.2.1 To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

6.2.2 The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

6.2.3 Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

6.2.4 All staff, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

6.2.5 The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it, and how they can support children who may be affected.

6.2.6 In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

6.2.7 The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7. EXAMINING ELECTRONIC DEVICES

7.1 School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

7.2 When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

7.3 If inappropriate material is found on the device, it is up to the staff member, in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police.

7.4 Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

7.5 Any complaints about searching for, or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

8. MANAGING EMAIL

- Staff will only use official school provided email accounts to communicate with pupils and parents, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Emails sent to external organisations should be written carefully before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.

- Staff should not use personal email accounts during school hours or for professional purposes.
- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Spam, phishing and virus attachments can make email dangerous. The school ICT provider ensures mail is virus checked (ingoing and outgoing), includes spam filtering and backs emails up daily.

9. USE OF DIGITAL AND VIDEO IMAGES

9.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

9.2 However, staff, pupils and parents/carers need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement procedures to reduce the likelihood of the potential for harm.

9.3 We gain parental permission for the use of digital photographs or video involving their child as part of the school agreement form when their child joins the school. This is a once in a school lifetime consent. Parents are required to inform the school if their consent changes.

9.4 We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.

9.5 When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, pupils are advised to be very careful about placing any personal photos on any ‘social’ online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

9.6 Staff sign the school’s Acceptable Use Agreement and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.

9.7 The school blocks/filters access to social networking sites or newsgroups, unless there is a specific approved educational purpose.

9.8 Staff are allowed to take digital/video images to support educational aims, but must follow school procedures concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

9.9 Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school intodisrepute.

9.10 Pupils 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 Trustees, parents or younger children as part of their ICT scheme of work.

9.11 Pupils 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, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

9.12 If specific pupil photos (not group photos) are used on the school website, or in other high profile publications, the school will obtain individual parental or pupil permission for its long termuse.

9.13 Pupils’ full names will not be used anywhere on a website, particularly in association with photographs.

10. MANAGING FILTERING

- The school’s broadband access will include filtering, appropriate to the age and maturity of pupils.
- The school will work with the school’s broadband team to ensure that filtering

procedures are continually reviewed.

- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the DSL who will then record the incident and escalate the concern as appropriate.
- The school filtering system will block all sites known to contain inappropriate information.
- Changes to the school filtering procedures will be risk-assessed by staff with educational and technical experience prior to any changes and where appropriate, with consent from the Senior Leadership Team.
- The school Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

11. WEBCAMS AND CCTV

- The school uses CCTV for security and safety. The only people with access to this are the headteacher, the business manager and the SSO's
- Notification of CCTV use is displayed at the front of the school. Please refer to the Information Commissioners Office (ICO) for further guidance and the school CCTV procedures. Notification of CCTV in operation is displayed on the school website and the schools' newsletter.

12. DATA PROTECTION

12.1 Personal data will be recorded, processed, transferred and made available according to the GDPR May 2018, which states that personal data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- kept no longer than is necessary;
- processed in accordance with the data subject's rights;
- secure;
- only transferred to others with adequate protection.

13. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

13.1 All pupils, parents, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

13.2 Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

13.3 We will monitor the websites visited by pupils, staff, volunteers, trustees and visitors (where relevant) to ensure they comply with the above.

13.4 More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

14. PUPILS USING MOBILE DEVICES IN SCHOOL

14.1 Pupils who walk alone to and from school are permitted to bring mobile devices into school. These should be handed into the class teacher on arrival to school.

15. STAFF WORKING REMOTELY

15.1 Staff must ensure that their device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

15.2 If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

16. STAFF USE OF PERSONAL DEVICES

- Mobile phones and personally owned devices will be switched off or switched to 'silent' mode.
- Bluetooth communication should be switched off and mobile phones or personally owned devices will not be used during teaching periods.
- Staff should not use personal devices, such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Where members of staff are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency

where a staff member does not 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.

- If a member of staff breaches the school policy and procedures then disciplinary action may be taken.

17. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

17.1 Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour and safeguarding policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

17.2 Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

17.3 The school will consider whether incidents, which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

18. TRAINING

18.1 All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

18.2 All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, and staff meetings).

18.3 The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

18.4 Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

18.5 Volunteers will receive appropriate training and updates, if applicable.

18.6 More information about safeguarding training is set out in our child protection and safeguarding policy.

19. LINKS WITH OTHER POLICIES

19.1 This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy.

APPENDIX 1: EYFS AND KS1 ACCEPTABLE USE AGREEMENT (PUPILS AND PARENTS/CARERS)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school, I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:

  I click on a website by mistake

  I receive messages from people I don't know

  I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

APPENDIX 2: KS2 ACCEPTABLE USE AGREEMENT (PUPILS AND PARENTS/CARERS)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the Acceptable Use Agreement Policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it
- **I will not:**
- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- **If I bring a personal mobile phone or other personal electronic device into school:**
- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
- **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

Signed (pupil):	**Date:**

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

ACCEPTABLE USE OF THE SCHOOL’S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Signed (parent/carer):	**Date:**

APPENDIX 3: ACCEPTABLE USE AGREEMENT (STAFF, TRUSTEES, VOLUNTEERS AND VISITORS)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

APPENDIX 4: ONLINE SAFETY TRAINING NEEDS – SELF AUDIT FOR STAFF

Adapt this form to suit your needs

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school’s acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school’s acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school’s ICT systems?	
Are you familiar with the school’s approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	