



Learn-AT

Learning ~ Fellowship

E-Safety Policy

LAT019 Version 3 Updated July 2022

Created by: DSL Group and J. Bladon
Approved by: Trustees (7th July 2022)
Next Review: July 2023

Table of Contents

1.	Aims.....	3
2.	Legislation and guidance.....	3
3.	Roles and responsibilities.....	3
4.	Educating pupils about online safety	6
5.	Educating parents about online safety	7
6.	Cyber-bullying	7
7.	Acceptable use of the internet in school.....	8
8.	Pupils using mobile devices in school	8
9.	Staff using work devices outside school	9
10.	Staff use of personal devices	9
11.	Email and Social Networking	10
12.	Copyright	10
13.	How the school will respond to issues of misuse	11
14.	Training.....	11
15.	Monitoring arrangements.....	11
16.	Links with other policies	11
	Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers)	13
	Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)	14
	Appendix 3: Online Safety Training Needs – Self-Audit For Staff.....	15
	Appendix 4: Online Safety Incident Report Log	16
	Appendix 5: Learn-AT Remote Learning Safeguarding Protocol for Parents	17
	Appendix 6: Learn-AT Remote Learning Safeguarding Protocol – Teaching Staff	19

Please note that this policy supersedes and replaces any equivalent policies or sections of policies. This policy is non contractual and can therefore be amended without consultation. Before you use this policy, please check you have the latest version using the footer reference and Learn-AT Policy Index.

This policy applies to all Learn Academies Trust schools and should be read in conjunction with the latest associated guidance issued by Learn- AT.

1. Aims

1.1. Learn-AT aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- 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 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](#).

2.2. 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 the Learn-AT funding agreement and articles of association.

3. Roles and responsibilities

The Learn-AT Trust Board

3.1. The Learn-AT Trust Board approves this policy and delegates responsibility for its implementation at individual academy level to the academies' Local Governing Bodies.

The Local Governing Bodies (LGB)

3.2. The LGBs have responsibility for monitoring this policy and holding headteachers to account for its implementation.

- 3.3. The LGB will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the academy's designated safeguarding lead (DSL). (Appendix 4)
- 3.4. Each school will appoint a Governor who oversees online safety
- 3.5. All local governors will:
 - Ensure that they have read and understand this policy
 - Agree and adhere to the terms on acceptable use of the school's IT systems and the internet and the Learn-AT Data Protection Policy

The headteacher

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

The designated safeguarding lead

- 3.7. Details of the school's designated safeguarding lead (DSL) are set out in the school's child protection and safeguarding policy.
- 3.8. 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, IT manager and other staff, as necessary, to address any online safety issues or incidents
 - Ensuring that any online safety incidents are logged (see appendix 4) 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 (appendix 3 contains a self-audit for staff on online safety training needs)
 - 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
 - Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- 3.9. This list is not intended to be exhaustive.

The IT Manager

- 3.10. The IT Manager is responsible for:
 - Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
 - Ensuring that the school's IT 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 IT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

3.11. This list is not intended to be exhaustive.

All staff and volunteers

3.12. 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 IT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

3.13. This list is not intended to be exhaustive.

Parents

3.14. 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 IT systems and internet (appendix 1)
- The agreement should be completed at each phase - **Y1, Y3 and Y5**. Teachers will go through the acceptable use agreement (appendix 1) in their first computing lesson, ask the children to sign it and then send home for parents to counter sign. Ensuring that children understand the school expectations.
In year 2, 4, and 6 teachers will review the agreement in the first lesson to remind the children and include any new starters.

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

- What are the issues? UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- NSPCC online safety advice: <https://www.nspcc.org.uk/keeping-children-safe/online-safety/>
- Net Aware NSPCC and O2: <https://www.net-aware.org.uk/>

- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>

Visitors and members of the community

- 3.16. Visitors and members of the community who use the school's IT 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 (appendix 2).

4. Educating pupils about online safety

- 4.1. Pupils will be taught about online safety as part of the curriculum.
- 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
 - How to report a range of concerns
- 4.4. The safe use of social media and the internet will also be covered in other subjects where relevant.
- 4.5. 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.
- 4.6. The following links are from Keeping Children Safe in Education and may be used within school:
- DfE advice for schools: teaching online safety in schools
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf
 - UK Council for Internet Safety (UKCIS)27 guidance:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf
 - National Crime Agency's CEOP education programme:
<https://www.thinkuknow.co.uk/>
 - Public Health England:
<https://campaignresources.phe.gov.uk/schools/topics/mental-wellbeing/overview> Rise Above

5. Educating parents about online safety

- 5.1. Each of the Learn Academies Trust schools will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.
- 5.2. Online safety will also be covered within parent communication.
- 5.3. 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.
- 5.4. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

Definition

- 6.1. 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 and anti-bullying policy.)

Preventing and addressing cyber-bullying

- 6.2. 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.
- 6.3. 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. Teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.
- 6.4. 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.
- 6.5. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
- 6.6. Each of the Learn Academies Trust schools will also send 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.
- 6.7. 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.
- 6.8. 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.

Examining electronic devices

- 6.9. 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.
- 6.10. 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
- 1.1. 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:
- 6.11. 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
- 6.12. Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).
- 6.13. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

- 7.1. All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
- 7.2. 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.
- 7.3. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
- 7.4. More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

- 8.1. Pupils may bring mobile devices into school, but are not permitted to use them

during the school day. Pupils who need mobile phones to communicate with their parents or carers for safety reasons on the way to and from school may leave their phones securely in the school office or another designated place during the school day and collect them at home-time.

- 8.2. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

- 9.1. Staff members using a work device outside school for work or personal use must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.
- 9.2. Staff may use work devices for reasonable personal use out of school hours (e.g. using the internet in line with this policy or checking personal email accounts). Email attachments must not be opened on a work device unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- 9.3. Personal files (e.g. photographs, music, documents) and passwords must not be stored on a work device. Staff are reminded that all files saved on their work device are synced with the server and that their work device may need to be handed in without prior notice for checking, repairs or updates.
- 9.4. School devices must not be used to upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others (e.g. child sexual abuse images, criminally racist material, adult pornography, material which incites hatred or discrimination, material which promotes gambling or any form of online risk-taking, material which is degrading to any individual or group).
- 9.5. Staff must ensure that their work device is secure, encrypted 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.
- 9.6. If staff have any concerns over the security of their device, they must seek advice from the IT manager.

10. Staff use of personal devices

- 10.1. Staff members must not use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on school trips.
- 10.2. All staff, volunteers and students must ensure that their mobile phones, personal cameras and recording devices are not used for personal use in school and are stored securely out of sight during working hours in teaching areas and any other area of the school where children are present. During Covid-10 staff may need to use their personal phones for reporting safeguarding instances (if Teams is not

available) please see Child Protection Addendum for further details. Mobile phones must not be used for making personal phone calls, texting, checking personal emails or accessing personal social media sites in any teaching area in school during lesson times or whilst children are present.

- 10.3. Mobile phones, iPads, iPods and any other portable devices must not be used in toilet or changing areas under any circumstances.
- 10.4. All telephone contact with parents or carers must be made using the school landline or mobile phone, not personal mobile phones.
- 10.5. Where possible, all school related work should be carried out on a work device. In the case were a personal computer or laptops is used, staff must ensure that no personal data or sensitive data is stored on that device.

11. Email and Social Networking

- 11.1. Staff members and governors must use the email address provided by the school for all school-related communication. Personal email addresses must not be used for school purposes and school emails must not be forwarded to a personal email account.
- 11.2. School email accounts must not be used for any personal communication not related to school.
- 11.3. School devices may not be used to access social networking sites for personal purposes on the school site but may be used to access and update the school's own social networking accounts.
- 11.4. Staff, students and volunteers are reminded that social networking sites should be regarded as public forums and as such any discussion about school issues, colleagues or pupils is strongly discouraged. Any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school will result in disciplinary action.
- 11.5. Staff members must make every effort to ensure that neither their personal/professional reputation, or the school's reputation is compromised by inappropriate postings on social media and must not disclose any confidential or sensitive information, or information or images that might compromise the security of the school.
- 11.6.
- 11.7. Staff members must not share personal information with a pupil (e.g. personal phone number or email address) or communicate with pupils via personal social networking accounts.

12. Copyright

- 12.1. Staff must ensure that they have permission to use the original work of others in their own or their pupils' work. Where work is protected by copyright (including music and videos), it must not be copied, downloaded or distributed without

permission from the copyright holder.

13. How the school will respond to issues of misuse

- 13.1. Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
- 13.2. Where a staff member misuses the school's IT 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.
- 13.3. Incidents which involve illegal activity or content will be reported to the police.

14. Training

- 14.1. 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.
- 14.2. 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, e-bulletins and staff meetings).
- 14.3. The DSL 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.
- 14.4. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- 14.5. Volunteers will receive appropriate training and updates, if applicable.
- 14.6. More information about safeguarding training is set out in our child protection and safeguarding policy.

15. Monitoring arrangements

- 15.1. The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.
- 15.2. This policy will be reviewed annually by the Trust's IT Manager and DSL Working Group. At every review, the policy will be approved by the Trust Board and adopted by all Learn-AT academies.

16. Links with other policies

- 16.1. This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Learn-AT School Use of Twitter

Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers)

The agreement should be completed at each phase - **Y1, Y3 and Y5**. Teachers will go through the acceptable use agreement (appendix 1) in their first computing lesson, ask the children to sign it and then send home for parents to counter sign. Ensuring that children understand the school expectations. In year 2, 4, and 6 teachers will review the agreement in the first lesson to remind the children and include any new starters.

Acceptable use of the school's IT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's computers or i-Pads and using the internet in school, I will not:

- Use them for anything other than for learning
- Use them when a teacher is not there, or without a teacher's permission
- Access any websites other than the sites the teacher has told us to use
- Access sites such as Facebook, Twitter unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms, (this is where you can talk to other people on the computer)
- Open any anything in emails, or follow any links that you can click on in emails, without first checking with a teacher
- Type any inappropriate language on the computer
- Share my password with others or use anyone else's computers details like their user name or password
- Give my information about me like my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Arrange on the computer to meet anyone in person/ at the park/ outside of school 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 leave it at the school office for safe-keeping and collect it at the end of the day.

I agree that the school will know the websites I visit.

I will immediately let a teacher or anyone that works at the school know if I see anything on the computer that upsets, distresses or might harm me or others.

I will always use the school's computer and internet responsibly.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's IT 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 IT 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: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

Acceptable use of the school's IT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

I have read and agree to abide by the school's E-Safety Policy.

I will only use the school's IT 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.

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 IT 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 IT systems and internet responsibly, and ensure that pupils in my care do so too.

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

Date:

Appendix 3: Online Safety Training Needs – Self-Audit For Staff

Online safety training needs audit	
Name of staff member/volunteer:	Date:
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 IT 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? Please record them here.	

Appendix 4: Online Safety Incident Report Log

Online safety incident report log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 5: Learn-AT Remote Learning Safeguarding Protocol for Parents

When children have to stay at home for self-isolation, our school will use Microsoft Teams to communicate with children, provide access to remote learning assignments, activities and recorded lessons and some live interaction with their teachers and classmates online. To keep children and staff safe there is a strict safeguarding protocol which everyone must follow very carefully.

All parents and carers must read the protocol below carefully and complete the online form at http://bit.ly/learnt_rl

Your child will only be able to access remote learning after you have confirmed that you will follow the procedures in this protocol.

Joining the Teams session

The teacher will set a day and time for the call and send an invitation to the children's Teams accounts via the Teams calendar

Your child will need to click on the 'Join' button in the Teams calendar to join the session at the set time

You should be able to join the call from a smartphone, tablet or laptop as long as it has a microphone and speaker.

Safeguarding Protocol

Children should be dressed in clothes suitable for school

Anyone else who might be seen on screen during the call must also be appropriately dressed (e.g. parents and carers, siblings)

Please make sure that your child joins the call in a shared area of your home, e.g. living room, dining room, kitchen, and not from a bedroom. A neutral background such as a plain wall would be ideal. If this is not possible please check the background behind your child to ensure that it is suitable to be visible to others on the call.

If you have any concerns about your child, family or home being seen on screen by others you may choose to turn off the camera for the call.

A parent or carer should remain in the room with the child while they are on the call but should not be visible on the screen or speak to the teacher or other children.

Language must be professional and appropriate, including any family members who might be heard in the background of the call.

All calls will be recorded for safeguarding and training purposes.

Videos will be kept for 21 days in case of any complaints or queries. They may also be shared with any member of the class who is not able to join the call 'live' to allow them to catch up at a later time.

Calls must not be recorded or screenshots taken by anyone other than the school.

Normal school rules will apply during the call including:

- being on time for the lesson

- behaving respectfully towards others
- following instructions
- listening to the teacher as they are talking.

Teachers may have to remove a child from the call if the rules above are not followed.

If the teacher has any safeguarding concerns during the call, these will be followed up in the usual way according to the school's Child Protection Policy.

Code of Conduct for Parents and Carers

Learn-AT's Social Media Code of Conduct for Parents and Carers (<https://www.learnat.uk/attachments/download.asp?file=72&type=pdf>) will apply to remote learning calls. In particular:

All Learn-AT schools expect parents and carers to behave in a respectful, civil and courteous way online and will not tolerate any of the following online behaviours:

Sending or posting abusive or unkind messages to or about parents or teachers

Posting anything negative or unkind about fellow parents, pupils, the school or its employees on social media

Complaining about the school's policies, values and methods on social media

We welcome constructive feedback, provided in the right way, either by email or in person to school staff. Teachers and school leaders are always happy to listen and talk to parents to address any concerns they may have. Complaints should be made following the guidance outlined in the Learn-AT Complaints Policy:

<https://www.learnat.uk/attachments/download.asp?file=71&type=pdf>

Behaviour on social media which is likely to damage the reputation of the school, the trust or any member of staff

This applies to any comments relating to anything to do with the teacher or other children that is observed during remote learning sessions and includes social media platforms, such as Facebook, Instagram, TikTok or Twitter, and messaging apps, such as WhatsApp.

Breaches of this code of conduct will be taken very seriously by the school and the trust. Breaches could lead to the school withdrawing access to online remote learning for the children of the family involved.

Posting illegal, defamatory, or discriminatory content could lead to prosecution.

Appendix 6: Learn-AT Remote Learning Safeguarding Protocol –

Teaching Staff

All staff involved in remote learning must read the protocol below carefully.

The staff code of conduct – Guidance for Safer Working Practices – May 2019 must always be adhered to.

<https://www.saferrecruitmentconsortium.org/GSWP%20Sept%202019.pdf>

Platform

All remote learning must take place via the MS Teams platform using only Learn-AT email addresses and login details.

Consent

Pupils can only take part in the remote learning sessions if the parents have given written consent. School offices will have a list of consents.

Teaching staff will also need to complete the form below to give their consent to take part in remote learning sessions: http://bit.ly/learnt_rlf

Remote Learning Protocol for parents and pupils

The Learn-AT Remote Learning Protocol for parents and pupils is shared with all parents and as part of their consent they will acknowledge that they agree to the code of conduct which states the following.

2.1. All Learn-AT schools expect parents and carers to behave in a respectful, civil and courteous way online and will not tolerate any of the following online behaviours:

Sending or posting abusive messages to parents or teachers

Sending or posting abusive messages about parents and teachers

Posting defamatory 'statuses' about fellow parents, pupils, the school or its employees

Complaining about the school's policies, values and methods on social media

(We welcome constructive feedback, but it should be provided through official channels either by email or in person to school staff. Complaints must be made following the guidance outlined in the Learn-AT Complaints Policy_

<https://www.learnat.uk/attachments/download.asp?file=71&type=pdf>

Any behaviour on social media which is likely to bring the reputation of the school, the trust or any member of staff into disrepute

This applies to any comments relating to anything regarding the teacher or other children that is observed during remote learning sessions and includes social media platforms, such as Facebook or Twitter, and messaging apps, such as WhatsApp.

Breaches of this code of conduct will be taken very seriously by the school and the trust. Breaches could lead to the school withdrawing access to online remote learning for the children of the family involved. Posting illegal, defamatory, or discriminatory content could lead to prosecution.

Staff who become aware of a breach of this code of conduct must inform school leaders immediately.

Live streaming

There are three situations where live lessons may be used for remote learning -

A child who is self-isolating may be invited to join their peers who are still at school for parts of lessons.

The whole class and staff are self-isolating, and the teacher is conducting live lessons from home.

In a local or national lockdown, the teacher may conduct live lessons from the classroom for pupils learning at home.

Timetables for remote learning sessions should be shared and agreed with school leaders.

To create a safe environment for children and young people when watching or engaging in a livestream, there are several things you should consider.

Ensure the background visible on screen is neutral and there is nothing of a personal nature visible e.g. family photographs. The 'background effects' settings can be used to blur the background or set a neutral background.

Calls should be made from a neutral space (e.g. study, dining room but not a bedroom).

Begin recording the lesson before the pupils arrive.

Have two adults participating in the session if possible.

Report any safeguarding concerns immediately following the school child protection policy.

Be aware of and make adjustments for any child with SEND to ensure that they are able to access live lessons.

Before starting any livestream, remind children:

- usual school rules apply during live lessons
- how they can ask questions during the session
- not to share private information
- not to respond to contact requests from people they don't know
- who they should tell if they see or hear anything upsetting or inappropriate?
- turn off their camera if their parents have asked them to.

Contacting parents

All audio calls to parents must be pre-arranged and conducted through MS Teams not a personal phone. The teacher can send a Teams meeting invitation to a parents via the Teams calendar.

Formal scheduled parents' meeting can be booked through the Parents' Meetings booking system (set up and used in the summer term).