Helping people living in extraordinary circumstances to live ordinary lives

Kingsley Learning Foundation Trust

Online Safety Policy

Chair Signature: *D. Withers*

Reviewed by Policy Working Group: **Autumn 2025**

Reviewed by Governors: **Autumn 2025**

Review Cycle: **1 Year**

Contents

1. Introduction 4

1.1 Aims 4

1.2 Legislation and guidance 4

1.3 Scope 4

2. Roles and responsibilities 5

2.1 The Governing Board 5

2.2 The Headteacher 5

2.3 The DSL/Online Safety Lead 5

2.4 ICT Support Service 6

2.5 All staff and volunteers 6

2.6 Guardians 6

2.7 Visitors and members of the community 6

3. Educating pupils about online safety 6

3.1 Delivery of online safety 6

3.2 What pupils will learn 6

4. Educating guardians about online safety 7

4.1 Guardian training and communications 7

4.2 Guardian concerns 7

5. Cyber-bullying 7

5.1 Definition 7

5.2 Preventing and addressing cyber-bullying 7

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. The school will actively discuss cyber-bullying with pupils (where appropriate), explaining the reasons why it occurs, the forms it may take and what the consequences can be. 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. 7

6. Examining electronic devices 8

6.1 Reasons to examine electronic devices 8

6.2 Responses to inappropriate material 8

7. Artificial Intelligence (AI) 8

7.1 Use of artificial intelligence 8

8. Acceptable use of the internet and devices 9

8.1 Internet agreement 9

8.2 Pupils using mobile phones and smartwatches in school 9

8.3 Staff using work devices 9

8.4 Staff using work devices outside school 9

8.5 Personal devices 9

9. How the school will respond to issues of misuse 10
9.1 Procedures following misuse by staff 10
9.2 Procedures following misuse by pupils 10
10. School systems 11
10.1 GDrive 11
10.2 Gmail 11
10.3 Zoom/Teams/Google Meet 11
10.4 Portable devices 11
10.5 Photos 12
10.6 Assessment system 12
10.7 ClassDojo 12
10.8 Communication 12
11. Training 12
11.1 New staff 12
11.2 All staff 12
11.3 DSL and DDSL 12
11.4 Governors and volunteers 12
11.5 Training content and aims 12
13. Monitoring arrangements 13
13.1 Monitoring of school network and use of ICT facilities 13
14. Equal opportunities 13

1. Introduction

1.1 Aims

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. At Kingsley Learning Foundation Trust (KLFT), we understand that computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of pupils and adults. Whilst exciting and beneficial to all in school, we need to be aware of the range of risks associated with the use of these technologies and want to ensure that all our pupils are safe when online and that clear expectations are in place for practices in school.
At KLFT we aim to:

- Ensure the safeguarding of all pupils within and beyond the school setting by detailing appropriate and acceptable use of all online technologies.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Outline the roles and responsibilities of everyone.
- Ensure adults are clear about procedures for misuse of any online technologies both within and beyond the school setting.
- Develop links with guardians to promote awareness of the benefits and potential issues related to technologies.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Overall, the purpose of this policy is to promote a culture of responsible and safe internet use in our school. We believe that by working together, we can create a safe and supportive online environment for all of our pupils. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk as stated within Keeping Children Safe in Education:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example, pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **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:** personal 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).
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. (DfE Keeping Children Safe in Education 2025)

1.2 Legislation and guidance

Accordingly, this policy is written in line with the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE'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.
The policy also takes into account the national curriculum computing program of study.
Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

1.3 Scope

This policy applies to all members of the KLF Trust community (including staff, the governing board, volunteers, contractors, pupils, guardians, visitors and community users) who have access to our digital

technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

2. Roles and responsibilities

This Trust is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour to protect staff, pupils, families and the reputation of each school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

2.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the Headteachers to account for its implementation.

The governing board will coordinate regular meetings with appropriate staff to discuss online safety and requirements for training and monitor online safety logs as provided by the designated safeguarding lead (DSL). The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet the school's safeguarding needs.

The governor who oversees online safety is Debbie Withers.

All governors will:

- Make sure that online safety is a running and interrelated theme when devising and implementing the whole school approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted to meet the needs of our learners. This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

2.2 The Headteacher

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

2.3 The DSL/Online Safety Lead

Details of the school's DSL's and deputies are set out in our Safeguarding and Child Protection Policy.

A DSL or Deputy DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that all staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher and Governing Board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Working with the Headteacher, ICT support service and other staff, as necessary, to address any online safety issues or incidents.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the ICT support service to make sure the appropriate systems and processes are in place.
- Ensuring that any online safety incidents (including cyber-bullying) are logged and dealt with appropriately in line with the Trust safeguarding/behaviour policy.
- Managing all online safety issues and incidents in line with the school's safeguarding policy.
- Updating and delivering staff training on online safety at least annually in order to continue to provide them with relevant skills and knowledge.
- 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.

2.4 ICT Support Service

The ICT support service are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness to 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 ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis.

2.5 All staff and volunteers

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

- Maintaining and understanding 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/Online Safety Lead to ensure that any online safety incidents (including cyber-bullying) are logged and dealt with appropriately.
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the Trust behavior policy.
- Knowing that the DSL/Online Safety Lead is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting to the DSL/Online Safety Lead.
- Responding appropriately to all reports and concerns about sexual violence and/or harassments, both online and offline, and maintaining an attitude of 'it could happen here'.

2.6 Guardians

Guardians are expected to:

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

Guardians 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
- Healthy relationships - Disrespect Nobody
- CEOP education

2.7 Visitors and members of the community

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.

3. Educating pupils about online safety

3.1 Delivery of online safety

Pupils will be taught about online safety regularly and specifically during their computing and PSED/PSHE sessions. Targeted sessions may also be offered to address any key issues that have been identified. The Trust also takes part in Safer Internet Day each year.

3.2 What pupils will learn

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 use other online technologies.

- Recognise acceptable and unacceptable behaviour.
- Develop stranger awareness.
- Identify a range of ways to report concerns about content and contact.
- How to consider the effect of their online actions on others and to know how to recognise and display respectable behaviour online and the importance of keeping personal information private.
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online.
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.

The safe use of social media and the internet will also be covered in other subjects where relevant.
NB. Teaching about safeguarding, including online safety, will be adapted to meet the needs of our learners.

4. Educating guardians about online safety

4.1 Guardian training and communications

The school will raise guardians' awareness of internet safety in letters or other home communications, and in information via our website or ClassDojo. The online safety lead will meet with individual families for support and advise if this is requested or identified as a need through safeguarding. This policy will be available for guardians on the school website.

4.2 Guardian concerns

If guardians have any queries or concerns in relation to online safety, these should be raised in the first instance with a member of class staff. Concerns or queries regarding this policy can be raised with any member of staff or a member of the senior leadership group.

5. Cyber-bullying

5.1 Definition

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.

5.2 Preventing and addressing cyber-bullying

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

All staff receive training on cyber-bullying, its impact and ways to support pupils as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Anti-Bullying 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. 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.

6. Examining electronic devices

6.1 Reasons to examine electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- There is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher/DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

6.2 Responses to inappropriate material

If inappropriate material is found on the device, it is up to the DSL/Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response. If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image.
- Confiscate the device and report the incident to the DSL (or DDSL) immediately, who will decide what to do next.

The DSL (or DDSL) will make the decision in line with the DfE's latest guidance on 'Screening, Searching and Confiscation' and the UK Council for Internet Safety (UKCIS) guidance on 'Sharing Nudes and Semi-Nudes: advice for education settings working with children and young people'.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the Police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the guardian refuses to delete the material themselves.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Behaviour Policy.

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. Artificial Intelligence (AI)

7.1 Use of artificial intelligence

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and guardians may be familiar with generative chatbots such as ChatGPT and Google Gemini.

The Trust recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography - pornographic content created using AI to include someone's likeness.

The Trust will treat any use of AI to bully pupils in line with our Anti-Bullying and Behaviour policies.
Staff should be aware of the risks of using AI tools; please see the Trust's Use of Artificial Intelligence by Staff in Schools policy for further information.

8. Acceptable use of the internet and devices

8.1 Internet agreement

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.
We will monitor the websites visited by pupils, staff, volunteers, Governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

8.2 Pupils using mobile phones and smartwatches in school

Pupils are advised to leave their mobile phones at home, however, if they are needed, for example, for regulatory purposes on transport, they must be handed over to reception until the end of the day. Our concerns are:

- Inappropriate or bullying text messages.
- Images or videos taken of adults or peers without permission being sought.
- Watching/accessing inappropriate content.

Smartwatches are allowed to be worn by pupils but these must be switched to airplane mode whilst the pupil is on the school site.

8.3 Staff using work devices

The KLFT provides technology for staff to use to fulfil the requirements of their role in school. There is also adequate equipment for staff to use within school. On receipt of the hardware, a laptop or iPad agreement is signed outlining the expectations of using the equipment.
To ensure all ICT equipment runs smoothly and efficiently staff are asked to complete the following actions once a term:

- Review their passwords ensuring they are secure. It is advised that passwords are at least 8 characters long and include a capital letter, lowercase letter, number and special character.
- Review their cloud storage and delete anything which is no longer needed or duplicates of items.
- Delete the emails in the deleted file on Gmail.
- Review the emails in other files and delete any no longer needed.
- Empty the computer's recycle bin.
- Delete the contents of the download folder.

Staff members must not use the device in any way which would violate the school's terms of acceptable use.
Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the IT Support Service or School Business Manager.

8.4 Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password protected – strong passwords are recommended including at least 8 characters, with a combination of upper- and lowercase letters, numbers and special characters.
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date – always install the latest updates.
- Using the cloud storage systems to store information/planning safely.
- Not storing personal information or sensitive materials on unencrypted and/or portable drives.

8.5 Personal devices

In the event that a member of staff needs to use their own equipment, they need to get permission from the Headteacher and ensure they follow the same security procedures as for school-owned equipment.

Staff must not use mobile phones in school during directed teaching time and these must be locked away. Phones are only to be used during staff breaks and in designated areas.
Smartwatches are allowed to be worn by staff, however, this must be switched to airplane mode during work hours (see Code of Conduct Policy).

9. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, the action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
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 Policy.
The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the Police.

9.1 Procedures following misuse by staff

The Headteacher will ensure that these procedures are followed in the event of any misuse of the internet by an adult:

A) An inappropriate website is accessed inadvertently:

- Identify and make a note of the URL of the website.
- Report website to the DSL if this is deemed necessary.
- Contact the filtering service for school so that it can be added to the banned or restricted list.
- Change Local Control filters to restrict locally.
- Check the filter level is at the appropriate level for staff use in school.

B) An inappropriate website is accessed deliberately:

- Identify and make a note of the URL of the website.
- Ensure that no one else can access the material by shutting down.
- Log the incident.
- Report to the Headteacher and DSL immediately.
- Headteacher to refer back to the acceptable use rules in this policy and follow agreed actions for discipline.
- Inform filtering services and the LA.

C) An adult receives inappropriate material:

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Headteacher immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice, e.g. Police.

D) An adult has used ICT equipment inappropriately:

- Follow the procedures in B.

E) An adult has communicated with a pupil or used ICT equipment inappropriately:

- Ensure the pupil is reassured and remove them from the situation immediately, if necessary.
- Report to the Headteacher and DSL immediately.
- Preserve the information received by the pupil if possible and determine whether the information received is abusive, threatening or innocent.
- Once procedures and policy have been followed and the incident is considered innocent, refer to the acceptable use rules for staff, and Headteacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and DSL immediately and follow the allegations procedure and Safeguarding policy.
- Contact CEOP (Police) as necessary (CLICK CEOP, TUK website).

F) Where staff or adults are posted on inappropriate websites, have posted inappropriate content, or have inappropriate information about them posted, this should be reported to the Headteacher.

9.2 Procedures following misuse by pupils

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the internet, by a pupil:

A) An inappropriate website is accessed inadvertently:

- Reassure the pupil that they are not to blame and praise them for being safe and responsible by telling an adult.
- Report website to the DSL if this is deemed necessary.
- Contact the helpdesk filtering service for school and LA so that it can be added to the banned list.
- Check the filter level is at the appropriate level for pupils use in school.

B) An adult or pupil has communicated with a pupil or used ICT equipment inappropriately:

- Ensure the pupil is reassured and remove them from the situation immediately.
- Report to the Headteacher immediately.
- Preserve the information received by the pupil if possible and determine whether the information received is abusive, threatening or innocent.
- Contact CEOP (Police) as necessary.

C) Threatening or malicious comments are posted on external websites about an adult in the school or setting:

- Preserve any evidence.
- Inform the Headteacher immediately.

N.B. Incidences that will be reported directly to the Police:

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

Indecent images: CEOP advice is to turn off the screen, secure the machine and contact the Police for further instructions if an indecent image is found. They will advise on how to deal with the machine if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine. Do not take a screenshot of the image. Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.

10. School systems

10.1 GDrive

Google Drive provides a secure cloud based suite of apps to facilitate collaborative working and central location to house documents for staff to remotely access. Each member of staff has a password for the suite linked to their email account which ensures the content is secure. Each member of staff has an area to save their individual working documents (MyDrive) and have access to shared drives which is our secure central location for storing documents which are accessible by staff with the appropriate permissions.

10.2 Gmail

All staff have an email account which is password protected. If secure emails are needed to be sent to external professionals which contain personal information these are sent using Egress and/or a password protected document. Emails should have an automated disclaimer which is designed to try and cover breaches of confidentiality, propagation of viruses, contractual claims and employee liability. Our disclaimer states:

DISCLAIMER: This email and its attachments may be confidential and are intended solely for the use of the individual to whom it is addressed. Any views or opinions expressed are solely those of the author and do not necessarily represent those of the KLF. If you are not the intended recipient of this email and its attachments, you must take no action based upon them, nor must you copy or show them to anyone.
Please contact the sender if you believe you have received this email in error.

10.3 Zoom/Teams/Google Meet

Zoom, Teams or Google Meet are used by staff within school for collaborative working, remote meetings, statutory review meetings with families and for remote learning. There is the facility to share documents and have a platform for team discussion.

NB: the KLFT has the infrastructure for personal data to be stored securely across Google Drive. Documents which contain personal data will not be stored on memory sticks or portable hard drives.

10.4 Portable devices

Across the school we use portable devices such as iPads and digital cameras to capture evidence of pupil's learning as a teaching and learning tool and to communicate with families via ClassDojo. These apps are selected and checked by the IT support service as well as monitored by the class teacher and team leaders.

10.5 Photos

As part of our school activities, we take photographs and record images of individuals within our school. We obtain written consent from guardians for photographs and videos to be taken of their child for communication, marketing and promotional materials. We clearly explain how the photograph and/or video will be used to both the guardian and pupil (where appropriate). Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns.
- Online on our school website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

10.6 Assessment system

We use Evidence for Learning (assessment website and app) to upload photos and videos as part of the system for recording pupil's learning. The data and evidence collated is stored on the schools iPads and desktop devices/school network and is uploaded securely via the Evidence for Learning app. Each staff member has a username and password to access the data stored on the website/app to prevent unauthorised access.

10.7 ClassDojo

We use ClassDojo as a platform to communicate with families. Both staff members and guardians login securely using a username and password and guardians must be added to the platform by the ClassDojo administrator to prevent unauthorised access. Photos/videos are uploaded securely to the ClassDojo portal and are shared either directly on a staff guardian private messaging system or via the whole class shared wall/story.

10.8 Communication

All electronic communications with pupils, guardians, employees and others are in line with the schools protocols using the appropriate means (school email, school telephone number, ClassDojo, school Zoom account). Personal details such as mobile number, social network details and personal details should not be shared or used to communicate with pupils and their families.

11. Training

11.1 New staff

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.

11.2 All staff

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

11.3 DSL and DDSL

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.

11.4 Governors and volunteers

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

Volunteers will receive appropriate training and updates, if applicable.

11.5 Training content and aims

Staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that pupils are at risk of online abuse.
- Pupils can abuse their peers online through:
    - Abusive, threatening, harassing, and misogynistic messages

- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
- Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

13. Monitoring arrangements

13.1 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This is primarily done through our firewall system which is monitored by our IT support service. This includes, but is not limited to, monitoring of:

- Internet sites visited.
- Bandwidth usage.
- Email accounts.
- User activity/access logs.
- Any other electronic communications.

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business.
- Investigate compliance with school policies, procedures and standards.
- Ensure effective school and ICT operation.
- Conduct training or quality control exercises.
- Prevent or detect crime.
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

Staff report behaviour and safeguarding issues relating to online safety and DSL will monitor, evaluate and follow up reports from staff.

This policy will be reviewed annually. At every review, the policy will be shared with the Governing Board.

14. Equal opportunities

We value the views of all persons in our school community. The school acts in the best interests of the pupils and their guardians to encourage high quality provision that meets diverse needs and promotes equality.