Part of T4 Trust

E-Safety Policy

Mobile Phone Safety

1. Version Control

Action	Name	Date
Prepared by	Lisa Tharpe	25.09.2021
Reviewed by	Lisa Tharpe	22.05.2022
Reviewed by	Lisa Tharpe	September 2022
Approved by	Local Governing Board	November 2022
Reviewed by	Lisa Tharpe	February 2023
Reviewed by	Lisa Tharpe	September 2023
Approved by	Trust Board	September 2023

Contents

Key contacts at IMHS

Trust Safeguarding and Compliance Reporting Lead:
Lisa Tharpe – Deputy Head (IMHS) - Email: lisa.tharpe@ianmikardo.com

The Designated Safeguarding Lead is:
Lynn St. Phillip-Ross – Lead Inclusion and Welfare Practitioner – Email: Lynn.st.phillip-ross@ianmikardo.com

The Deputy Safeguarding Officers are:
Aaron Mulhern – Executive Headteacher - Email: aaron.mulhern@ianmikardo.com
Hazera Begum- Attendance and Welfare Coordinator - Email: Hazera.begum@ianmikardo.com
Karen Raftery – Head of Post 16 and Careers - Email: karen.raftery@ianmikardo.com
Jason Levine – Designated Mental Health Lead – Email: jason.levine@ianmikardo.com

The Safeguarding Leads - Board of Governors for T4 Trust are:
Helal Ahmed – Local Community Board of Governor for Safeguarding
Sara Attwood – T4 Trust Board of Governor for Safeguarding

IT Support
IT Support Provider - NS Optimum Limited - **Tel:** – 01926 880300 (ext. 420)
Mobile – 07973116063 **Email:** technical@nsoptimum.co.uk

IT Access Monitor - David Lightman Media, Teacher - **Email:** david.lightman@ianmikardo.com
Tel: 020 8981 2413

We believe this policy should be a working document that is fit for purpose, represents the school ethos, enables consistency and quality across the school and is related to the following legislation:

- Obscene Publications Act 1959
- Children Act 1989
- Computer Misuse Act 1990
- Education Act 1996
- Education Act 1997
- Police Act 1997
- Data Protection Act 2018
- Human Rights Act 1998
- Standards and Framework Act 1998
- Freedom of Information Act 2000
- Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Children and Young Persons Act 2008
- School Staffing (England) Regulations 2009
- Equality Act 2010
- Education Act 2011
- Protection of Freedoms Act 2012
- Counter Terrorism and Security Act 2015

- Education Act 2003

The Following Documentation is Also Related to This Policy:

- Dealing with Allegations of Abuse against Teachers and other Staff: Guidance for Local Authorities, Headteachers, School Staff, Governing Bodies and Proprietors of Independent Schools (DfE)
- Equality Act 2010: Advice for Schools (DfE)
- Keeping Children Safe in Education: Statutory Guidance for Schools and colleges (DfE)
- Prevent Strategy (HM Gov)
- Teaching approaches that help build resilience to extremism among people (DfE)
- Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children
- Race Disparity Audit - Summary Findings from the Ethnicity Facts and Figures Website (Cabinet Office)

We believe we have a duty to provide students with quality Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills.

We believe that when used correctly, Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the school's management information and business administration systems.

We acknowledge that the increased provision of the Internet in and out of school brings with it the need to ensure that learners are safe. We need to teach students how to evaluate Internet information and to take care of their own safety and security.

It is essential that students are safeguarded from potentially harmful and inappropriate online material. There are many online safeguarding issues that can be categorised into four areas of risk:

Content:	Being exposed to illegal, inappropriate, or harmful material such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
Contact:	Being subjected to harmful online interaction with other users such as 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 such as making, sending, and receiving explicit images.
Commerce:	Risk such as online gambling, inappropriate advertising, phishing and of financial scams

E-Safety, which encompasses Internet technologies and electronic communications, will educate students about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.

We believe all students and other members of the school community have an entitlement to safe Internet access at all times.

We work hard to increase parents' understanding of the internet and of the serious safeguarding issues and risks that there are for children online and how to keep them safe.

We have a duty to safeguard children, young people, and families from violent extremism. We are aware that there are extremists' groups within our country who wish to radicalise vulnerable children and to involve them in terrorism or in activity in support of terrorism. Periodic risk assessments are undertaken to assess the risk of students being drawn into terrorism. School staff must be aware of the increased risk of online radicalisation, and alert to changes in students' behaviour. Any concerns will be reported to the Designated Safeguarding Lead.

We are aware that under the 'Counterterrorism and Security Act 2015' we have the duty to have 'due regard to the need to prevent people from being drawn into terrorism'. This duty is known as the Prevent duty and we believe it is essential that school staff are able to identify those who may be vulnerable to radicalisation or being influenced by extremist views, and then to know what to do when they are identified.

We provide a safe environment where we promote students' welfare. Within this environment we work hard to build students' resilience to radicalisation and extremism by promoting fundamental British values and for everyone to understand the risks associated with terrorism. We want students to develop their knowledge and skills in order to challenge extremist views.

We as a school community have a commitment to promote equality and believe this policy is in line with the Equality Act 2010.

We all have a responsibility to ensure equality permeates into all aspects of school life and that everyone is treated equally irrespective of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation. We want everyone connected with this school to feel safe, secure, valued and of equal worth.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that are connected with this policy.

2. Aims

- To provide students with quality Internet access as part of their learning experience across all curricular areas
- To provide clear advice and guidance in order to ensure that all Internet users are aware of the risks and the benefits of using the Internet
- To evaluate Internet information and to take care of their own safety and security
- To raise educational standards and promote student achievement
- To protect children from the risk of radicalisation and extremism
- To ensure compliance with all relevant legislation connected to this policy
- To share good practice within the school, with other schools/school and with the local authority in order to improve this policy

Educating students about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All secondary schools have to teach:

Relationships and sex education and health education in secondary schools

Students will be taught:

To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.

How to report a range of concerns

By the **end of secondary education**, students will know:

- Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content

- That specifically sexually explicit material (e.g., pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared, and used online
- How to identify harmful behaviours online (including bullying, abuse, or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

Where necessary, teaching about safeguarding, including online safety will be adapted for vulnerable children, victims of abuse and some students with SEND.

Responsibility of the Policy and Procedure

3. Role of the Governing Body

The Local Governing Board has:

- Appointed a member of staff to be responsible for e-Safety
- Delegated powers and responsibilities to the Headteacher to ensure all school staff and stakeholders are aware of and comply with this policy
- Responsibility for ensuring that the school complies with all equality's legislation
- Responsibility for ensuring funding is in place to support this policy
- Responsibility for ensuring this policy and all policies are maintained and updated regularly
- Make effective use of relevant research and information to improve this policy
- Responsibility for ensuring policies are made available to parents
- Undertaken training in order to understand e-Safety issues and procedures

- ☐ Determining this policy with the Local Governing Board
- ☐ Discussing improvements to this policy during the school year
- ☐ Organising surveys to gauge the thoughts of all students
- ☐ Reviewing the effectiveness of this policy with the Local Governing Board
- ☐ Visit the school regularly
- ☐ Work closely with the Headteacher and the School Leadership team
- ☐ Ensure this policy and other linked policies are up to date

- ☐ Ensure that everyone connected with the school is aware of this policy
- ☐ Attend training related to this policy
- ☐ Report to the Local Governing Board every term
- ☐ Annually report to the Local Governing Board on the success and development of this policy

Responsibility for the effective implementation, monitoring and evaluation of this policy.

4. Role of the Executive Headteacher

The Executive Headteacher will:

- Ensure the safety and e-Safety of all members of the school community
- Work in conjunction with the School Leadership Team to ensure all school staff, students and parents are aware of and comply with this policy
- Work closely with the Local Governing Board and School leadership Team to create a safe ICT learning environment by having in place

  - ☐ An effective range of technological tools
  - ☐ Clear roles and responsibilities
  - ☐ Safe procedures
  - ☐ A comprehensive policy for students, staff and parents

- Ensure risk assessments are:

  - ☐ In place and cover all aspects of this policy in order to reduce internet misuse
  - ☐ Accurate and suitable
  - ☐ Reviewed annually
  - ☐ Easily available for all school staff

- Ensure all new programme's will be installed onto the network or standalone machines by NS Optimum
- Ensure personal CD's and other data record devices may not be used in school
- Ensure everyone must be aware that under the Computer Misuse Act 1990 the use of computer systems without permission or for inappropriate use could constitute a criminal offence
- Ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Embed e-Safety in all aspects of the curriculum and other school activities
- Investigate, record and report all infringements to e-safety by any member of staff or by a student
- Deal with all complaints of Internet misuse by staff or students
- Ensure all students and staff must read and sign the 'Acceptable ICT Use Agreement' before using any school IT resource
- Ensure parents sign a consent form before their child has access to the Internet
- Ensure an up-to-date record is kept of all students and school staff who have Internet access

- Inform parents if their child has misused the Internet
- Ensure a safe and secure username / password system is in place for all

☐ Technical systems
☐ Networks
☐ Devices and Email and Virtual Learning Environments ensure secure passwords are regularly changed by using Password Generator (https://passwordsgenerator.net/);

- Ensure passwords for new school will be allocated by using Password Generator (https://passwordsgenerator.net/)
- Ensure replacement passwords for existing school staff will be allocated by using Password Generator (https://passwordsgenerator.net/)

Ensure all users are responsible for:

☐ The security of their username and password
☐ Not allowing other users to use this information to access the system
☐ Reporting any suspicion or evidence that there has been a breach of security
☐ Changing their password at regular intervals by using Password Generator (https://passwordsgenerator.net/)

- Deal with all breaches of security
- Impose the appropriate sanctions to any infringement of e-Safety
- Will immediately suspend a member of staff if they commit an exceptionally serious act of gross misconduct
- Will immediately suspend and report to the Police if images of child abuse are found on a computer belonging to a member of staff
- Ensure any inappropriate websites or material found by students or a member of staff will be reported to the e-Safety DSL and IT Access Monitor who in turn will report to the Internet Service Provider
- Ensure the school website complies with current DfE guidelines
- Ensure the following will not be published on the school's website

☐ Staff or students contact details
☐ The pictures of children without the written consent of the parent/carer
☐ The names of any students who are shown
☐ Student's work without the permission of the student or the parent/carer

Organise a series of safeguarding and child protection workshops to ensure parents are aware of:

☐ Keeping Children Safe in Education: Statutory Guidance for Schools and colleges
☐ Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children
☐ The Safeguarding and Child Protection policy
☐ Safeguarding procedures in place
☐ All safeguarding policies

- ☐ Their role in safeguarding and child protection

- Provide leadership and vision in respect of equality
- Make effective use of relevant research and information to improve this policy
- Provide guidance, support and training to all staff
- Monitor the effectiveness of this policy by:

- ☐ Monitoring learning and teaching through observing lessons
- ☐ Monitoring planning and assessment
- ☐ Speaking with students, school, parents, and governors

- Annually report to the Governing Body on the success and development of this policy

5. Role of the e-Safety IT Access Monitor/DSL

The IT Access Monitor /DSL will:

- Be responsible for the day-to-day e-Safety issues
- Undertake an annual e-safety audit in order to establish compliance with guidance for the DFE and T4 Trust
- Ensure that all Internet users are kept up to date with new guidance and procedures
- Have editorial responsibility of the school website and will ensure that content is accurate and appropriate
- Ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Maintains a log of all e-Safety incidents
- Reports all e-Safety incidents to the Headteacher
- Ensure e-Safety is embedded in all aspects of the curriculum and other school activities
- Organise e-Safety workshops for parents/carers in order to:

  - ☐ Increase their understanding of the internet;
  - ☐ Discuss the serious safeguarding issues and risks for children online and how to keep them safe;

- Coordinate short e-Safety presentations developed by students that they will present at school events
- Regularly update the school website with e-safety information for parents
- Send e-safety text messages to parents every term
- Write a brief account of e-Safety in regular newsletters
- Develop a progressive internet safety curriculum for the whole school
- Ensure all new school are aware of and sign the Acceptable Use Agreement
- Ensure all students understand the Online Acceptable Use Agreement before signing

- Ensure all parents are aware of and sign the Acceptable Use Agreement
- Lead the development of this policy throughout the school
- Work closely with the Headteacher and the Local Governing Board
- Make effective use of relevant research and information to improve this policy
- Provide guidance and support to all staff
- Provide training for all staff on induction and when the need arises
- Keep up to date with new developments and resources
- Review and monitor
- Annually report to the Local Governing Board on the success and development of this policy.

The Designated Safeguarding Lead

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

In relation to the KCSIE 2023 update, there is emphasis on filtering and monitoring systems and standards, there is added clarification that the Designated Safeguarding Lead has chief responsibility for this within their school/college.

Governing bodies and proprietors have also been specified as responsible members for ensuring "all staff undergo safeguarding and child protection training" which includes the new outlines of filtering and monitoring systems. This training should be regularly updated, as in line with KCSIE 2023.

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 staff and consultants and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- 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 4 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 Headteaacher and/or governing board

6. Role of School Staff

School staff will:

- Comply with all aspects of this policy
- Undertake appropriate training
- Before using any Internet resource in school must accept the terms of the 'Responsible Internet Use' statement
- Not allow others to use their log on details
- Report any suspicion or evidence that there has been a breach of security
- Teach students the importance of password security
- Be responsible for promoting and supporting safe behaviours with students
- Promote e-Safety procedures such as showing students how to deal with inappropriate material
- Report any unsuitable website or material to the IT Access Monitor and DSL
- Will ensure that the use of Internet derived materials complies with copyright law
- Ensure e-Safety is embedded in all aspects of the curriculum and other school activities
- Be aware of all other linked policies
- Maintain high standards of ethics and behaviour within and outside school and not to undermine fundamental British values
- Work in partnership parents and carers keeping them up to date with their child's progress and behaviour at school
- Implement the school's equalities policy and schemes
- Report and deal with all incidents of discrimination
- Attend appropriate training sessions on equality
- Report any concerns they have on any aspect of the school community

7. Role of Students

Students must be taught to:

- Be critically aware of the materials they read
- Validate information before accepting its accuracy
- Acknowledge the source of information used
- Use the Internet for research
- Respect copyright when using Internet material in their own work
- Only use approved e-mail accounts
- Report receiving any offensive e-mails
- Not divulge their or others personal details
- Not arrange to meet anyone via the e-mail
- Seek authorisation to send a formal e-mail to an external organisation
- Not take part in sending chain letters
- Report any unsuitable website or material to the e-Safety lead.

Know and understand the school policy on the use of:

- ☐ Mobile phones
- ☐ Digital cameras
- ☐ Handheld devices

Know and understand the school policy on the taking and use of photographic images and cyber bullying and not be allowed access to:

- ☐ Social networking sites except those that are part of an educational network or approved Learning Platform
- ☐ News groups unless an identified need has been approved

- Develop and present short e-Safety scenarios to parents at school events
- Learn to take pride in their work
- Produce work of a high standard
- Listen carefully to all instructions given by the teacher
- Ask for further help if they do not understand
- Participate fully in all lessons
- Participate in discussions concerning progress and attainment
- Treat others, their work and equipment with respect
- Support the school Code of Conduct and guidance necessary to ensure the smooth running of the school
- Talk to others without shouting and will use language which is neither abusive nor offensive
- Hand in homework properly completed and on time
- Take part in questionnaires and surveys

8. Role of Parents/Carers

Educating Parents/Carers About Online Safety

The school will raise awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during “parents’ days”.

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.

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

Parents/carers will:

- Be aware of and comply with this policy
- Be asked to support the e-Safety policy and to sign the consent form allowing their child to have Internet access
- Make their children aware of the e-Safety policy
- Be invited to attend e-Safety workshops in order to discuss the serious safeguarding issues and risks to children online and how to keep them safe
- Be encouraged to take an active role in the life of the school by attending

  - ☐ Parent open days
  - ☐ Parent-teacher consultations
  - ☐ School Events
  - ☐ Fundraising and social events

- Be asked to take part periodic surveys conducted by the school
- Ensure regular and punctual attendance
- Notify school on the first day of student absence
- Have holidays in term time and authorised by school
- Encourage effort and achievement
- Support the school Code of Conduct and guidance necessary to ensure smooth running of the school

9. Internet Filtering and Use

We have a contract with a reputed and national Internet provider to manage a secure and filtered Internet service which enables us to safely access and use the Internet and all email.

NS Optimum provides - IMHS with daily support for all IT Support queries and assistance.

The Internet filtering service will be annually reviewed.

Access to the Internet is designed to protect students and staff by blocking the following content:

- ☐ Adult content containing sexually explicit images
- ☐ Violent content containing graphically violent images
- ☐ Hate material content promoting violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
- ☐ Illegal drug taking content relating to the use or promotion of illegal drugs or the misuse or prescription drugs
- ☐ Criminal content relating to the promotion of criminal and other activities
- ☐ Gambling content relating to the use of online gambling websites
- ☐ Non educational websites such as social networking sites

All users access the Internet in accordance with the school's Acceptable Internet Use & Agreement and will inform the IT Access Monitor and DSL if at any time they find they have accessed inappropriate Internet sites.

When inappropriate material has been accessed the Internet Service Provider will be contacted and if necessary, liaise with Safer School's Police Officer.

10. Raising Awareness of This Policy

We will raise awareness of this policy via:

- School induction pack
- School website
- Staff induction pack
- Meetings with parents such as introductory, transition, parent-teacher consultations and periodic curriculum workshops
- school events
- Meetings with staff
- Written communications with home such as newsletters and of end of half term
- Annual report to parents
- Headteacher reports to the Local Governing Board
- Information displays in the main school entrance and around the school
- Text messages
- Email

11. Training

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.
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).

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

We ensure:

- All school staff:

  - ☐ Have received the appropriate training on all safeguarding policies and procedures undertaken by a registered training provider
  - ☐ Are familiar with the following documentation:

    - Keeping Children Safe in Education: Statutory Guidance for Schools and colleges
    - Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children

  - ☐ Are aware of the following linked policies:

- All aspects of this policy
- Safeguarding and Child Protection
- Acceptable Internet Use Agreement
- GDPR
- Behavior and Anti-bullying policy
- Online Cyber Procedures
- School Website
- Mobile Phone Safety and Acceptable Use

- The content of all training is correct, delivered well and engages staff as we believe that the more engaging training is, the better the outcomes that we need to measure
- That we have in place data that evidences staff understanding by using a simple short multiple-choice test through one of the following applications such as, Microsoft Forms, SSS training and The Key and TES training

- That we have in place evidence for all staff that:

  - ☐ Highlights the knowledge gaps in the training
  - ☐ Shows how those knowledge gaps were corrected
  - ☐ LGFL "**Undressed**" - a website that features a video and song that schools can use to teach young children about the risk of being tricked into getting undressed online

- All staff understand and undertake their role in safeguarding and child protection effectively

12. Safeguarding

We are committed to safeguarding and promoting the welfare of all students as the safety and protection of children is of paramount importance to everyone in this school. We work hard to create a culture of vigilance and at all times we will ensure what is best in the interests of all children.

We believe that all students have the right to be safe in our society. We recognise that we have a duty to ensure arrangements are in place for safeguarding and promoting the welfare of children by creating a positive school atmosphere through our teaching and learning, welfare support for both students and school staff, training for staff and with working with parents. We teach all our students about safeguarding.

We work hard to ensure that everyone keeps a careful watch throughout the school and in everything we do for possible dangers or difficulties. We want all of our students to feel safe at all times. We want to hear their views of how we can improve all aspects of safeguarding and from the evidence gained we put into place all necessary improvements.

Visitors and Members of the Community

Visitors and members of the community who use the school 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 policy.

Staff Using Work Technology Devices Outside School

Staff members using a work device outside school 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.

Staff must ensure that their work 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.

If staff have any concerns over the security of their device, they must seek advice from the IT Access Monitor and DSL.

Work devices must be used solely for work activities.

13. Online Safety

Students should have the right to explore the digital environment but also the right to be safe when on it. However, technology often provides the platform that facilitates harm, and the use of technology has become a significant component of many safeguarding issues. Examples of which include child sexual

exploitation; child criminal exploitation; radicalisation; sexual predation/grooming; and forms of child-on-child abuse.

In many cases abuse will take place concurrently via online channels and in daily life. Students can also abuse their peers online, which can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

Ian Mikardo High School aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community
- School community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

This policy is to be read in conjunction with all other policies for Ian Mikardo High School with particular emphasis on the need to understand the Safeguarding and Child Protection Policy, Behaviour and Anti-Bullying Policy and Staff Code of Conduct. With detailed safeguarding procedures, including raising and reporting concerns for young people and staff. Please also see the Home Guide on how to use Microsoft Teams and internet safety advice.

How The School Will Respond to Issues of Misuse

Where a student misuses the schools ICT systems or internet, we will follow the procedures set out in our behaviour and anti-bullying policy. 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 procedures and staff code of conduct. 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.

The 4 Key Categories of Risk

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk that should form the framework for school's approach to Online Safety:

- **Content:** being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racism, prejudice-based content, 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 as well as adults posing as children or young adults with the intention of grooming or exploiting 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 or 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. When pupils are at risk of phishing, school can report concerns to the Anti-Phishing Working Group (https://apwg.org/)

Cyber-bullying

Cybercrime is a criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).
When there are concerns about a child in this area, staff should notify the DSL, who will consider referring the child into the Cyber Choices programme (cyberchoices.uk), which provides early intervention where students are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Safeguarding of students extends to the online environment. All Staff are aware of the risks posed to students by technology and the internet, and should understand their role in preventing, identifying, and responding to harm caused by its use. Abuse can take place wholly online or technology may be used to facilitate offline abuse.

The school has adopted a whole-school approach to online safety which captures the range and complexity of the risks and of students' experiences of those risks; seeks to mitigate those risks as far as possible without depriving students of the significant benefits provided by technology and the internet; and handles all cases of online harm appropriately and with sensitivity. In particular, this policy sets out the risks posed to students by the internet and technology, the indicators that a child may be at risk of such harm, and the measures taken by the school to mitigate these risks, including student and parent

education, staff training, and limiting the risk of harm caused by the School's IT systems (e.g.: appropriate filters). Further to this, it includes reference to the use of mobile technologies, including the management of access to 3G / 4g and 5G through mobile devices.

The Senior Leadership Team and relevant staff should have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when they are identified and in particular those who are potentially at greater risk of harm.

The DSL and will together with NS Optimum and the IT Access Monitor to ensure measures are in place and action is taken along with online safety auditing annually.

Students Using Mobile Devices in School

Students may bring mobile devices into school but are not permitted to use them during lessons.

Any use of mobile devices in school by students must be in line with the acceptable use agreement and our Behaviour & Anti-bullying policy.

Any breach of the acceptable use agreement by a student may trigger further action in line with the school behaviour policy, which may result in the device being collected by a parent or carer.

All staff must report Online Safety concerns about students to the Designated Safeguarding Lead as with all other safeguarding concerns. When it comes to the safety and well-being of the child, the response to the risks and harms that students may experience in the online or digital environment should be no different than the offline, face to face world.

For most students there is little distinction between online and face to face interactions as the two environments often intersect with one another in their daily lives. Staff should recognise that students' experience of abuse in the digital environment may be even more pronounced, where the identity of the abuser is unknown and the abuse can continue 24 hours a day, 7 days a week.

In relation to online safety, the KCSIE 2023 now places an expectation that the Local Governing Board hold this as a central theme in their whole setting approach to safeguarding.

14. Students Safety When Working from Home

The Internet offers many opportunities and importantly helps us to support our students in their learning. However, the internet also presents some risks to users and therefore parents and carers should take precautions to help protect their child.

How Will You Know That the Work Being Set Has Come From a Child's Teacher?
All work for Student will be set using Microsoft Teams Online Classroom If students are asked to do something that has not been set through Teams Online Classroom, it has not come from a member of staff at IMHS. Some teachers may signpost Student within Teams Online Classroom to websites or apps, but the Microsoft Teams Online Classroom will always be the starting point.

How Will We Communicate with Students?
We have asked staff to ensure all communication with students is done through Microsoft Teams - Online Classroom and via phone. No communication with students from a teacher will be made using private email accounts.

Using Additional Online Platforms and Online Private Tuition at Home

We are aware that some parents and carers may wish to engage with private tutors online or additional learning tools beyond that recommended by the school. If you do make this decision, please look for recommendations from other families before you begin. We recommend that all students engaging with any online platforms should be in an area of the house where adults are present so you can confirm the interaction is appropriate.

What Should Students Do if They Want to Report Abuse on the Internet?

If student experiences abuse online during school hours, they can contact a member of SLT or the Welfare Team via "Microsoft Teams".

- Ms. Karen Raftery (Deputy Safeguarding Lead)
- Mr. Aaron Mulhern (Headteacher)
- Mrs. Lisa Tharpe (Trust Safeguarding & Compliance Reporting Lead)
- Ms. Lynn St Phillip-Ross (Designated Safeguarding Lead)
- Ms. Hazera Begum (Deputy Designated Safeguarding Lead)

If Student wish to access support from external agencies, we would recommend:

- Childline - for support
- UK Safer Internet Centre - to report and remove harmful online content
- CEOP - for advice on making a report about online abuse

Additional Information for Supporting Students on the Internet

These nationally recognised websites have valuable resources for parents and carers to use:

- Internet matters - for support for parents and carers to keep their children safe online
- London Grid for Learning - for support for parents and carers to keep their children safe online
- Net-aware - for support for parents and carers from the NSPCC
- Parent info - for support for parents and carers to keep their children safe online
- Thinkuknow - for advice from the National Crime Agency to stay safe online
- UK Safer Internet Centre - advice for parents and carers
- Child net - has produced a Parent and Carer Toolkit which is a collection of three resources designed to help you talk to your young person about their online life, manage boundaries around family internet use and point you in the direction of where to get further help and support.
- NSPCC Net Aware - provides a useful guide to social networks, apps and games.

For further information, please refer to the following;

- Keeping children/young people safe online guidance
- IMHS home guide's "how to utilise TEAMs- Student guidance

Our school has established clear and distinct policies to ensure the safety and well-being of our students in the digital age. Our Behaviour & Ant-bullying Policy outlines our expectations for responsible behaviour in both online and offline environments. Alongside this, our Acceptable Use Agreement for staff and students outlines the guidelines and responsibilities for using digital devices and the internet within our setting. In recognition of the prevalent use of personal devices, we have a Mobile Phone and Smart Technology Policy that governs the use of mobile phones whilst on school premises. This policy also highlights how we manage student's access to the internet via 4G or 5G connections.

We are committed to maintaining a safe online environment, and as such, we conduct ongoing risk assessments and regular reviews of our Online Safety and cyber security practices. Our policies and practices are continuously refined to reflect the evolving digital landscape. Through these comprehensive measures, we aim to provide a secure and responsible digital experience for all our students, staff, and volunteers.

Risk Assessments
Each student will have a completed risk assessment (see appendix for template) in place regarding access to the internet and use of technology, and this must be reviewed each term. The risk assessment must be personalised for each student, considering the specific needs of the student and the risks posed to them. It is the responsibility of the Key worker in partnership of the Tutor and DSL to ensure that appropriate risk assessments are in place and are reviewed regularly.

These assessments should be shared with relevant people, including where appropriate the student and their parents/carers to ensure clarity and a unified approach. These risk assessments must balance risk against benefit and not unnecessarily restrict a student's access to digital technology.

The risk assessments need to be approved by the Deputy Head; the school's IT Access Monitor will then advise NS Optimum (IT Support Provider) of the specific access needs of each student. NS Optimum will then be able to ensure that each student has access and permissions set up for their user profile.

Web Content Filtering
IMHS is subscribed to LGFL to ensure our web content filters are up to date and effective with the support of NS Optimum which is the school's IT support provider. This means that we do not actively block web content ourselves.

We only block content in the following categories on our corporate network:

- Known malicious sites
- Gambling
- Unsecure shopping sites
- Pornography
- Terrorism and violence
- Adult offensive content
- Bullying

If you find a legitimate web page necessary for your daily tasks that are filtered, you will have the opportunity to request for this page to be unblocked.

If you plan to use a website as part of a lesson or presentation, check in advance to ensure that the site is not filtered. NS Optimum is not always able to respond to unblock requests at short notice and can therefore not guarantee that a site will be available when needed.

If anyone should discover unfiltered content that they deem to be unsafe, malicious, or offensive they should report this to the IT Access Monitor so that this can be added to our web filter.

Staff are asked to inform the IT Access Monitor of any such sites that either need to be explicitly blocked or explicitly allowed. We will amend the relevant policies as required after assessment of the site.

Profiles may be changed temporarily as a result of a specific concern or misuse of them by an individual (s). Staff must inform the DSL and the IT team when they have concerns about a student accessing inappropriate and / or harmful material. The school will take reasonable measures to prevent access to inappropriate materials. However, due to the global nature of the internet and its content, it is not always possible to guarantee that such material will never appear on any computer. In the event that such materials are accessed, these must be reported to the IT Access Monitor and DSL so that these sites may be added to the filtered list. Certain sites and programmes are deemed prohibited (due to being illegal) and will not be available to any user.

Web Monitoring

On a weekly basis the DSL will liaise with NS Optimum advisor to generate a report of anyone (student, staff, volunteer and visitor) who has or has tried to access sexually explicit material, illegal material or anything that could be attempting to radicalise others. Where concerns are raised through this, they are then managed under the school's disciplinary procedure. This information is then shared with the Headteacher.

Teaching, Learning and Welfare Team

The Teaching, Learning and Welfare Team are responsible for the day-to-day planning, reviewing and management of the students' education both in and out of the classroom, the tutor / teacher and Keyworker for each student must ensure that:

A risk assessment for each student is carried out and communicated to all relevant members of staff where appropriate, parents and carers are informed of the outcome of the risk assessment and the impact of this on the student's access is explained. Staff in their area are fully aware of their responsibility and how to implement the policy through training and guidance.

The IT Access Monitor is informed of the outcome of this process and advised as to access requirements for each student. Students are supervised and the appropriate services informed of any breaches of the policy.

15. Equality

Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation.

We believe that our policy is in line with the Equality Act 2010.

16. Race Disparity Audit

We acknowledge the findings of the Race Disparity Audit that clearly shows how people of different ethnicities are treated across the public services of health, education, employment, and the criminal justice system.

17. Monitoring the Implementation and Effectiveness of the Policy

The practical application of this policy will be reviewed annually or when the need arises by the DSL/IT Access Monitor, the Headteacher and the Local Governing Board.
The DSL will log behaviour and safeguarding issues related to online safety. All online incidents are incidents are recorded on MyConcern.

A statement of the policy's effectiveness and the necessary recommendations for improvement will be presented to the Local Governing Board or the Trust Board for further discussion and endorsement.

18. Linked Policies and Agreements

- Safeguarding and Child Protection
- Acceptable Internet Use Agreement
- Behaviour and Anti-bullying
- School Website
- Mobile Phone Safety and Acceptable Use

We Believe This Policy:

- Has been reviewed thoroughly by the safeguarding governor and the Designated Safeguarding Lead has been questioned on it to make sure it stands up to scrutiny
- Flows and is easy to follow
- Is an essential part of the school
- Supports staff in managing certain situations
- Forms an important framework that will ensure consistency in applying values and principles throughout the establishment

- Provides guidance, consistency, accountability, efficiency, and clarity on how the school operates
- Provides a roadmap for day-to-day operations
- Ensures compliance with laws and regulations, gives guidance for decision-making, and streamlining internal processes
- Is designed to influence and determine all major decisions, actions and all activities taking place within the boundaries set by them
- Stems from the school's vision and objectives which are formed in strategic School Leadership meetings
- Has been received by all school staff via appropriate safeguarding training

Example 1

Data Protection, Security and Social Media Agreement (Student)

We hope you will enjoy using the school's computers to support your learning in all your lessons. Please sign this agreement to let us know that you understand your responsibilities when you use the school's computers and Internet.

I, _____ agree that:

- I will use the school's computers and access the Internet in school only for educational purposes related to my school studies. I will not use the computers to buy or sell goods.
- I will never tell anyone else my password, and never use someone else's logon name or password.
- I will always get permission from a member of staff before I download anything and won't install or store programmes on the computer without consent from staff.
- I won't use a removable device like a CD or USB flash drive on the computers without consent.
- I will not use, or attempt to use, social media like Facebook, snap chat or Instagram when in school.
- If I use social media outside of school, I will not post messages that could be offensive to students or staff at the school.
- I will not attempt to access Internet sites or music that contain material that is inappropriate for school (Music or images related to illegal things, drugs or gang activity)
- I will not attempt to access areas of the school's computer system beyond the access given me by the school.
- I will not attempt to access staff computers (desktops/laptops).
- I understand that staff are able to look at my files and communications to make sure that I am using the system responsibly.
- I understand that if I damage the operation of the school's computers or computer system, use the Internet inappropriately, or attempt to hack into the system outside my access, I may be no longer be able to use the school's computers and police might be involved.
- I will never eat or drink near ICT equipment.

I confirm that I have read and understand the above:

Student Signed: _____ Date: _____

Parent/Carer Signed: _____ Date: _____

Example 2

Ian Mikardo High

Mobile Phone Contract (Student)

Mobile phone contract between _____ and Ian Mikardo High School

This is to confirm that I understand that the use of mobile phones, PSPs and tablets is restricted in school.
I understand that if I bring any of this equipment to school:

- I cannot use it during lessons.
- I cannot use it to play loud music in school.
- If I use my phone, PSP or tablet inappropriately, I must hand it in to the school Office and collect it at the end of the day.
- If I refuse to hand in my phone, PSP or tablet, the school will phone my parent or carer who will be asked to come to school immediately to collect the equipment.
- If I continue to use my phone, PSP or tablet inappropriately, my parent or carer will be asked to ensure that I do not bring them to school or might be asked to collect it.
- It is my responsibility to look after my mobile phone, PSP and/or tablet in school. Should any of these devices go missing, the school will not be held responsible.

Student Signed: _____ Date: _____

Parent/Carer Signed: _____Date: _____

School Staff Signed: _____Date: _____

Example 3

Online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Example 4

Online safety training needs – self audit for staff

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's	
Do you know what you must do if a student 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 students and parents/carers?	
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?	

This policy must be read in conjunction with the schools Online Cyber Safety Procedures.