



**Inspiring Futures
through Learning**

Inspiring Futures through Learning

Online Safety Policy

September 2026 to September 2027

Policy name:	IFtL Online Safety Policy
Version:	V3
Date relevant from:	September 2026
Date to be reviewed:	September 2027 <i>This policy will be reviewed annually unless legislation dictates otherwise. Recent changes in Legislation will need to be read and used to review this Policy.</i>
Role of reviewer:	IFtL Head of Safeguarding, Health, Children & Families, Head of Quality Assurance, Head of System Leadership
Statutory (Y/N):	Y
Published on website*:	1B

Policy level**:	1
Relevant to:	All employees through all IFtL schools and departments
Bodies consulted:	Employees Trade unions School / department governance bodies
Approved by:	IFtL Board of Trustees
Approval date:	

Key:

*** Publication on website:**

IFtL website

School website

1	Statutory publication	A	Statutory publication
2	Good practice	B	Good practice
3	Not required	C	Not required

**** Policy level:**

1. Trust wide:

- This one policy is relevant to everyone and consistently applied across all schools and Trust departments with no variations.
 - *Approved by the IFtL Board of Trustees.*
- 2. Trust core values:
 - This policy defines the values to be incorporated fully in all other policies on this subject across all schools and Trust departments. This policy should therefore form the basis of a localised school / department policy that in addition contains relevant information, procedures and / or processes contextualised to that school / department.
 - *Approved by the IFtL Board of Trustees as a Trust Core Values policy.*
 - *Approved by school / department governance bodies as a relevantly contextualised school / department policy.*
- 3. School / department policies
 - These are defined independently by schools / departments as appropriate
 - *Approved by school / department governance bodies.*

Contents

1. Purpose, Philosophy and Scope	5
2. Policy Leadership and Responsibilities	6
2.1 Shared Responsibility for Online Safety	6
2.2 Trustees	6
2.3 Local Governing Bodies	6
2.4 Executive Leaders and Senior Leaders	7
2.5 Designated Safeguarding Lead (DSL)	7
2.6 IFtL IT Team	8
2.7 Teaching and Support Staff	8
2.8 Pupils	9
2.9 Parents and Carers	9
2.10 Visitors, Volunteers and Community Users	10
3. Online Safety Education	10
4. Acceptable Use and Digital Behaviour	11
5. Reporting and Responding to Online Safety Concerns	12
6. Technology, Filtering, Monitoring and Cyber Security	14
7. Artificial Intelligence (AI)	17
8. Data Protection and Information Security	19
9. Digital Communications, Social Media and Online Publishing	20
10. Mobile Phones and Personal Devices	22
11. Remote Learning and Online Platforms	23
12. Training and Continuous Professional Development (CPD)	24
13. Monitoring, Review and Evaluation	26
14. Linked Policies, Procedures and Guidance	28

1. Purpose, Philosophy and Scope

Technology is an integral part of children's everyday lives and plays a central role in education, communication, creativity and learning. Digital technologies provide significant opportunities for pupils and staff; however, they also present safeguarding, wellbeing, privacy and cybersecurity risks that require a proactive, whole-school approach.

At IFtL, online safety is recognised as an essential component of safeguarding and child protection. The Trust is committed to ensuring that all members of the school community can use technology safely, responsibly and confidently, while developing the knowledge, skills and critical thinking required to navigate an increasingly complex digital world.

This policy sets out the Trust's approach to promoting safe and responsible use of technology through:

- effective online safety education;
- clear roles and responsibilities;
- robust safeguarding procedures;
- appropriate filtering and monitoring arrangements;
- secure management of digital systems;
- effective cyber security measures; and
- a culture where everyone understands their contribution to keeping children and young people safe online.

As a Multi-Academy Trust, IFtL operates a shared responsibility model for online safety. Individual schools retain responsibility for safeguarding practice, online safety education and responding to concerns involving their pupils. The Trust provides strategic oversight, technical infrastructure, cyber security support, assurance processes and specialist expertise through the IFtL IT Team.

This policy applies to all members of the IFtL community, including pupils, staff, governors, trustees, volunteers, parents/carers, visitors and community users who access school systems, digital services or technology provided by IFtL schools.

It applies to the use of technology:

- on school premises;
- when accessing school systems remotely;
- when using school-owned devices;
- when using personal devices on school sites where permitted; and
- where online activity outside school impacts on the safety, wellbeing or behaviour of members of the school community.

The Trust recognises that online safety extends beyond internet access and includes all forms of digital interaction, including websites, email, messaging services, social media, online gaming, livestreaming, connected devices and emerging technologies such as Artificial Intelligence (AI).

The Trust is committed to ensuring that digital systems are secure and resilient against cyber threats, whilst ensuring pupils are equipped with the knowledge, skills and understanding needed to make informed decisions, recognise online risks, seek support and participate positively in digital society.

2. Policy Leadership and Responsibilities

2.1 Shared Responsibility for Online Safety

Online safety is a shared responsibility across IFtL. All members of the Trust community have a role in promoting safe, responsible and respectful use of technology and in recognising, reporting and responding to concerns.

Online safety forms part of the Trust's wider safeguarding arrangements. The Designated Safeguarding Lead (DSL) retains lead responsibility for safeguarding, including online safety, within each school. The Trust provides strategic oversight, professional support, technical infrastructure and specialist expertise to support schools in meeting their statutory responsibilities.

Where online safety concerns arise, schools will respond in accordance with the IFtL Child Protection and Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct and other relevant procedures.

2.2 Trustees

Trustees provide strategic oversight and assurance that effective online safety arrangements are in place across the Trust.

Trustees will:

- ensure that online safety is recognised as part of the Trust's safeguarding responsibilities;
- ensure appropriate policies, systems and processes are in place to support safe use of technology;
- provide challenge and scrutiny regarding online safety arrangements, including filtering and monitoring, cyber security and safeguarding risks;
- receive appropriate assurance reports regarding online safety practice, significant incidents, emerging risks and improvement activity;
- ensure that appropriate safeguarding training is undertaken, including awareness of online safety responsibilities;
- provide assurance that the Trust has appropriate arrangements in place to meet relevant legislation, statutory guidance and regulatory expectations.

2.3 Local Governing Bodies

Local Governing Bodies provide challenge and oversight of online safety arrangements within their school.

Governors will:

- ensure that online safety is considered within the school's safeguarding arrangements;
- understand their responsibilities in relation to online safety, filtering and monitoring, and cyber security;
- receive appropriate information from school leaders regarding online safety risks, incidents, themes and actions;

- challenge whether online safety education, reporting procedures and technical safeguards are effective;
- ensure that the school is meeting the expectations of [Keeping Children Safe in Education](#) and relevant DfE guidance.

The nominated safeguarding governor should:

- maintain regular communication with the DSL regarding safeguarding themes, including online safety;
- understand the school's filtering and monitoring arrangements and how effectiveness is reviewed;
- receive appropriate assurance regarding staff training, pupil education and incident management;
- support effective challenge and continuous improvement.

2.4 Executive Leaders and Senior Leaders

Executive leaders and senior leaders are responsible for ensuring that online safety is embedded within the culture, practice and safeguarding arrangements of IFtL schools.

Senior leaders will:

- ensure that online safety is treated as an essential safeguarding responsibility;
- ensure that appropriate policies, procedures and systems are implemented effectively;
- ensure that staff receive appropriate safeguarding and online safety training, including understanding their responsibilities regarding filtering and monitoring;
- ensure pupils receive age-appropriate education about online safety and digital citizenship;
- work with DSLs and the IFtL IT Team to review the effectiveness of filtering and monitoring arrangements;
- ensure appropriate oversight of online safety incidents, themes and emerging risks;
- ensure that concerns involving staff are managed in accordance with safeguarding procedures and the staff disciplinary framework where appropriate.

2.5 Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for safeguarding and child protection within the school, including online safety.

The DSL will:

- understand the risks associated with online safety, including harmful content, online abuse, child-on-child abuse, exploitation, misinformation, AI-generated content and other emerging technologies;
- maintain knowledge and understanding of the school's filtering and monitoring systems and processes;

- coordinate safeguarding responses to online safety concerns;
- ensure concerns are recorded, assessed and managed in line with safeguarding procedures;
- liaise with senior leaders, governors, the IFtL IT Team and external agencies where required;
- contribute to the review of filtering and monitoring effectiveness;
- analyse patterns and themes from online safety concerns to inform education, training and preventative work;
- ensure pupils with additional vulnerabilities, including those with SEND, receive appropriate support.

The DSL may delegate specific operational tasks relating to online safety to appropriately trained staff; however, overall safeguarding responsibility remains with the DSL.

2.6 IFtL IT Team

The IFtL IT Team provides central technical support, infrastructure management and specialist expertise to enable schools to maintain secure and safe digital environments.

The IFtL IT Team will:

- maintain secure digital systems, networks and devices;
- implement and maintain filtering and monitoring solutions;
- support schools in understanding filtering and monitoring reports, alerts and technical information;
- provide advice regarding cyber security, system vulnerabilities and emerging technical risks;
- ensure appropriate access controls, authentication and security measures are implemented;
- support incident response where technical investigation is required;
- maintain awareness of relevant DfE technical standards and cyber security expectations;
- work collaboratively with DSLs and leaders to ensure technical controls support safeguarding practice.

Where technical services are provided centrally, individual schools remain responsible for safeguarding decisions and responding to concerns involving their pupils.

2.7 Teaching and Support Staff

All staff have a responsibility to promote safe and responsible use of technology and to contribute to a positive online safety culture.

Staff will:

- follow this policy, the Child Protection and Safeguarding Policy, Staff Code of Conduct and Acceptable Use Agreement;

- model safe, respectful and professional online behaviour;
- supervise pupils' use of technology appropriately;
- report online safety concerns promptly to the DSL;
- support pupils to understand online risks and responsible digital behaviour;
- teach pupils how to evaluate online information, recognise misinformation and use digital content ethically;
- protect confidential information and follow data protection requirements;
- use approved digital platforms and AI tools responsibly;
- complete required safeguarding and online safety training.

2.8 Pupils

Pupils are expected to use technology safely, responsibly and respectfully.

Pupils will:

- follow the school's acceptable use expectations;
- treat others respectfully online and offline;
- report concerns, harmful content or inappropriate behaviour;
- understand that online actions can have real-world consequences;
- protect their own and others' privacy;
- use digital content, including AI tools, ethically and responsibly;
- understand that behaviour outside school may be addressed where it affects members of the school community.

2.9 Parents and Carers

Parents and carers are important partners in supporting children to use technology safely.

IFtL schools will:

- share online safety information and guidance;
- provide access to relevant policies and acceptable use expectations;
- communicate emerging online risks where appropriate;
- signpost families to trusted sources of advice and support.

Parents and carers are encouraged to:

- discuss online safety regularly with their children;
- support responsible use of devices and online services;
- report concerns to the school where online activity impacts on pupil safety or wellbeing.

2.10 Visitors, Volunteers and Community Users

Visitors, volunteers and community users accessing IFtL systems or technology must comply with relevant acceptable use expectations and safeguarding requirements.

Access to systems will only be provided where appropriate safeguards are in place.

3. Online Safety Education

Online safety education is a fundamental part of the Trust's safeguarding curriculum and is embedded across school life. In line with [Keeping Children Safe in Education 2026](#), online safety is recognised as a running and interrelated theme within safeguarding practice and is reflected throughout the curriculum and wider safeguarding arrangements.

The Trust is committed to ensuring that pupils develop the knowledge, skills and confidence to use technology safely, responsibly and respectfully, both in school and beyond.

Online safety education will be:

- age-appropriate, inclusive and responsive to pupils' needs and vulnerabilities;
- delivered progressively throughout a pupil's education;
- embedded across the curriculum, including Computing, Relationships Education, Relationships and Sex Education (where applicable), PSHE and other relevant subjects;
- reinforced through assemblies, pastoral support, safeguarding activities and wider school life.

Pupils will be taught to:

- recognise and respond safely to online risks;
- understand the four areas of online risk (the 4Cs): **content, contact, conduct and commerce**;
- identify online abuse, bullying, grooming, coercion, exploitation and harmful online behaviour;
- understand consent, healthy online relationships and respectful communication;
- think critically about information they encounter online, including misinformation, disinformation and manipulated content;
- understand how Artificial Intelligence (AI) may generate inaccurate, biased or misleading content and develop the skills to evaluate AI-generated information critically;
- protect their personal information, privacy and digital identity;
- understand the importance of reporting concerns and know how to seek help;
- use technology legally, ethically and responsibly, including respecting copyright and intellectual property.

The Trust will ensure that online safety education reflects emerging technologies, current safeguarding risks and local or national issues identified through safeguarding practice, filtering and monitoring, pupil voice and wider intelligence.

Where appropriate, learning will be adapted to meet the needs of individual pupils, including those with SEND or other identified vulnerabilities.

Schools will work in partnership with parents and carers to promote safe online behaviours and provide access to information, guidance and resources that support children beyond the school environment.

4. Acceptable Use and Digital Behaviour

Technology plays an important role in teaching, learning and school life. The Trust expects all members of the IFtL community to use digital technologies safely, responsibly, respectfully and lawfully.

Acceptable use arrangements support the Trust's safeguarding responsibilities, protect the security of Trust systems and promote a positive digital culture.

All users of Trust technology are expected to:

- use digital technologies in ways that support learning, safeguarding and the wellbeing of others;
- behave respectfully and responsibly when communicating or interacting online;
- protect personal information, passwords and confidential data;
- use only authorised systems, devices, software and online services for Trust business;
- report online safety concerns, inappropriate content, security incidents or suspected misuse promptly;
- comply with relevant legislation, including data protection, copyright and intellectual property requirements;
- understand that misuse of Trust systems or technology may result in disciplinary action or other appropriate sanctions.

Staff

All staff, volunteers and contractors are expected to model safe and professional digital behaviour at all times.

Staff will:

- comply with the IFtL Staff Code of Conduct and Staff Acceptable Use Agreement;
- maintain appropriate professional boundaries when communicating electronically;
- use Trust-approved systems, platforms and AI tools for school business;
- protect confidential information and follow all data protection requirements;
- supervise pupils' use of technology appropriately;
- report safeguarding or cyber security concerns without delay;
- understand that Trust systems and devices may be monitored to ensure security, compliance and safeguarding.

Pupils

Pupils are expected to use technology safely, respectfully and responsibly.

Pupils will:

- follow the school's Pupil Acceptable Use Agreement and expectations for

responsible digital behaviour;

- use school technology for educational purposes unless otherwise authorised;
- respect the rights, privacy and wellbeing of others;
- protect their own accounts, passwords and personal information;
- report anything online that makes them feel worried, unsafe or uncomfortable;
- understand that online behaviour outside school may be addressed where it affects the safety, wellbeing or reputation of members of the school community.

Parents and Carers

Parents and carers are important partners in promoting safe technology use.

The Trust will provide information and guidance to support families in understanding online safety risks and expectations.

Parents and carers are encouraged to:

- reinforce safe and responsible online behaviour at home;
- support their child in following school expectations for technology use;
- report concerns to the school where online activity impacts on the safety or wellbeing of pupils.

Monitoring of Trust Systems

To help safeguard pupils, protect Trust systems and investigate concerns, the use of Trust-owned devices, networks and digital services may be monitored in accordance with legal requirements, Trust policies and the Trust's filtering and monitoring arrangements.

Users should have no expectation of privacy when using Trust-owned systems or devices for school purposes.

Acceptable Use Agreements

Detailed expectations for the use of Trust technology are set out within the Trust's Acceptable Use Agreements (AUAs), which apply to staff, pupils, governors, volunteers, visitors and other authorised users as appropriate.

These agreements are reviewed regularly to reflect changes in technology, legislation and safeguarding guidance and form part of the Trust's wider online safety framework.

5. Reporting and Responding to Online Safety Concerns

The Trust is committed to creating a culture in which all members of the school community feel confident and supported to report online safety concerns.

Online safety concerns may arise within or outside school and may involve pupils, staff, parents or members of the wider community. Where an online incident affects the safety, welfare or wellbeing of a pupil, it will be managed in accordance with the Trust's Child Protection and Safeguarding Policy and relevant statutory guidance.

All concerns will be taken seriously, assessed promptly and responded to proportionately, taking account of the age, vulnerability and needs of those involved.

Reporting concerns

All members of the school community are expected to report concerns about online safety without delay.

Concerns may include, but are not limited to:

- online bullying or harassment;
- child-on-child abuse occurring online;
- grooming or suspected exploitation;
- inappropriate contact from adults or other children;
- exposure to harmful, illegal or inappropriate content;
- the creation, sharing or possession of nude or semi-nude images;
- sextortion or online coercion;
- radicalisation or extremist material;
- hate incidents or discriminatory abuse;
- misuse of Artificial Intelligence (AI);
- cyber security incidents that may place individuals or Trust systems at risk;
- any online behaviour that causes concern for a child's safety or wellbeing.

Pupils will be regularly reminded how to report concerns and reassured that they will be listened to, supported and taken seriously.

Staff must report safeguarding concerns immediately to the Designated Safeguarding Lead (DSL) or a Deputy DSL in accordance with the Trust's safeguarding procedures.

Concerns relating primarily to the security of Trust systems must also be reported to the IFtL IT Team without delay. Safeguarding concerns will always remain the responsibility of the DSL.

Responding to concerns

All online safety concerns will be assessed on an individual basis.

The response will be proportionate to the nature of the concern and may include:

- safeguarding intervention;
- pastoral support;
- education and restorative approaches;
- behaviour management;
- technical investigation;
- referral to external agencies;
- criminal investigation where appropriate.

Where concerns indicate that a child may be suffering or likely to suffer harm, the school's safeguarding procedures will be followed immediately.

The school will work with parents and carers where appropriate, unless doing so would place a child at increased risk of harm.

Where necessary, the school will work collaboratively with external agencies including Children's Social Care, Police, Local Safeguarding Partnerships, the Internet Watch Foundation (IWF), CEOP and other relevant organisations.

Recording concerns

All safeguarding concerns relating to online safety will be recorded using the Trust's safeguarding recording system, CPOMs.

Records will include:

- the nature of the concern;
- actions taken;
- decisions made;
- agencies involved;
- outcomes and follow-up actions.

Information will be shared on a need-to-know basis and managed in accordance with safeguarding and data protection requirements.

Learning from incidents

The Trust recognises that online safety incidents provide valuable opportunities to strengthen safeguarding practice.

Schools will review trends and themes arising from incidents to:

- identify emerging risks;
- inform curriculum planning;
- review filtering and monitoring arrangements;
- identify staff training needs;
- strengthen safeguarding practice across the Trust.

Where appropriate, anonymised information may be shared with senior leaders, governors and trustees to support effective oversight and continuous improvement.

6. Technology, Filtering, Monitoring and Cyber Security

The Trust is committed to providing a secure digital environment that supports teaching, learning and safeguarding whilst protecting pupils, staff and Trust systems from online harm and cyber threats.

Effective technical safeguards are an important part of the Trust's wider safeguarding arrangements and complement, but do not replace, effective education, supervision and professional judgement.

Technology Infrastructure

The Trust provides centrally managed digital infrastructure, networks, devices and systems to support education and school operations.

The IFtL IT Team is responsible for maintaining secure and resilient technology systems across the Trust and works collaboratively with schools to ensure that technical controls support safeguarding and educational needs.

Schools remain responsible for the safeguarding of pupils and for responding appropriately to concerns identified through technical systems.

Filtering and Monitoring

In accordance with [Keeping Children Safe in Education 2026](#) and the [Department for Education Filtering and Monitoring Standards](#), the Trust has appropriate filtering and monitoring arrangements in place to help safeguard children and staff when using Trust technology.

Filtering and monitoring arrangements form part of the Trust's wider safeguarding approach and complement, but do not replace, effective online safety education, supervision and professional judgement.

Filtering

Filtering systems are used to prevent access to illegal, inappropriate or harmful content and are configured proportionately to support safeguarding whilst enabling access to appropriate educational resources.

The Trust's filtering arrangements are designed to:

- protect users from accessing illegal, inappropriate or harmful content;
- reduce the risk of exposure to online harms;
- support safe and effective use of digital technologies for teaching and learning;
- balance safeguarding requirements with the need for appropriate access to educational resources.

The Trust recognises that no filtering system can guarantee that all harmful content will be blocked. Filtering arrangements are therefore supported by effective supervision, online safety education and clear reporting procedures.

Monitoring

Monitoring systems are used to identify concerning activity, including potential safeguarding risks, and support timely intervention.

Monitoring arrangements may identify:

- attempts to access inappropriate or harmful content;
- indicators of safeguarding concerns;
- inappropriate use of Trust systems;
- potential cyber security risks.

Information identified through monitoring systems will be assessed appropriately and, where necessary, responded to through safeguarding, behaviour, disciplinary or technical procedures.

The Trust recognises that monitoring must be proportionate and balanced with privacy, data protection and the effective use of technology.

Review and Assurance

The effectiveness of filtering and monitoring arrangements is reviewed regularly to ensure that systems remain appropriate, effective and aligned with safeguarding requirements.

Reviews will involve appropriate representatives, including:

- senior leaders;
- the Designated Safeguarding Lead (DSL);
- the IFtL IT Team;
- governors and trustees where appropriate.

Reviews will consider:

- whether filtering systems are working effectively;
- whether monitoring arrangements identify relevant safeguarding concerns;
- whether systems remain appropriate for the needs of pupils and staff;
- whether staff understand their roles and responsibilities;
- whether improvements or changes are required.

Records of filtering and monitoring checks, reviews, decisions and actions will be maintained by the Trust in accordance with the Trust's governance and safeguarding arrangements.

Roles and Responsibilities

The Trust has clearly defined responsibilities for filtering and monitoring.

The IFtL IT Team is responsible for the technical implementation, maintenance and ongoing management of filtering and monitoring systems. The Trust will ensure that appropriate staff know how to access, interpret and act upon filtering and monitoring information.

The Designated Safeguarding Lead (DSL) is responsible for understanding how filtering and monitoring systems support safeguarding practice, reviewing safeguarding concerns arising from monitoring information and ensuring appropriate action is taken where concerns are identified.

Senior leaders provide strategic oversight and ensure filtering and monitoring arrangements remain effective, proportionate and compliant with statutory guidance.

Governors and Trustees receive appropriate assurance that filtering and monitoring arrangements are operating effectively.

Cyber Security

The Trust recognises that cyber security is an essential part of safeguarding and organisational resilience.

Appropriate technical and organisational measures are implemented to reduce the risk of cyber incidents affecting pupils, staff, digital systems and educational provision.

These measures include, where appropriate:

- secure user authentication and access controls;
- device and software management;
- network security and malware protection;
- secure backup and disaster recovery arrangements;
- vulnerability management and system updates;
- incident response and recovery procedures;
- staff awareness and cyber security training.

Cyber security arrangements are reviewed regularly to reflect emerging threats, changes in technology and national guidance.

Technical Incidents

Any suspected cyber security incident, system vulnerability or technical compromise must be reported immediately to the IFtL IT Team.

Where a technical incident presents a safeguarding risk, the IFtL IT Team will work alongside the Designated Safeguarding Lead and senior leaders to ensure both the technical and safeguarding aspects are managed appropriately.

Where required, incidents will be escalated in accordance with the Trust's incident management, safeguarding and data protection procedures.

7. Artificial Intelligence (AI)

Artificial Intelligence (AI), including generative AI, is becoming increasingly embedded within education. The Trust recognises that AI can enhance teaching, learning and school operations when used appropriately, whilst also presenting safeguarding, ethical, privacy and data protection risks that must be carefully managed.

The Trust supports the responsible use of AI in education where it is lawful, safe, transparent and aligned with educational outcomes. The use of AI must never replace professional judgement or safeguarding decision-making.

Principles

The Trust will ensure that the use of AI:

- supports teaching, learning and school improvement whilst promoting the safety and wellbeing of pupils;
- complies with relevant legislation, statutory guidance and the Trust's Data Protection and AI policies;
- is subject to appropriate human oversight;
- protects personal, confidential and commercially sensitive information;
- is regularly reviewed as technology and associated risks continue to evolve.

Staff Use of AI

Staff may use Trust-approved AI tools to support professional practice where this is appropriate and proportionate.

Staff must:

- exercise professional judgement when using AI-generated content;
- verify the accuracy, suitability and reliability of AI outputs before use;
- ensure that AI-generated content is appropriate for pupils and the intended purpose;
- avoid entering personal, confidential or sensitive information into AI systems unless explicitly authorised and compliant with Trust policies;
- comply with the Trust's Artificial Intelligence Policy, Data Protection Policy and Acceptable Use Agreement.

AI should support, rather than replace, professional expertise, decision-making or safeguarding responsibilities.

Pupil Use of AI

Where AI is used to support learning, pupils will receive age-appropriate education about its benefits, limitations and potential risks.

Pupils will be taught to:

- use AI responsibly, ethically and honestly;
- critically evaluate AI-generated content;
- recognise that AI outputs may be inaccurate, biased or misleading;
- acknowledge the appropriate use of AI within their learning;
- understand the importance of academic integrity and avoiding plagiarism.

Staff will provide appropriate supervision when AI tools form part of teaching and learning activities.

Safeguarding and AI

The Trust recognises that AI may increase safeguarding risks, including:

- AI-generated misinformation and disinformation;
- manipulated or synthetic images, audio and video (including deepfakes);
- AI-enabled grooming, exploitation and coercion;
- AI systems, including chatbots, that simulate human interaction and may create risks relating to emotional dependency, inappropriate content or exploitation;
- the creation or sharing of harmful or inappropriate content.

These risks will be addressed through online safety education, appropriate filtering and monitoring, staff training and safeguarding procedures.

Any safeguarding concerns involving AI will be managed in accordance with the Trust's Child Protection and Safeguarding Policy.

Governance and Review

The Trust will monitor developments in AI and review its approach regularly to ensure that emerging opportunities and risks are managed appropriately.

Further guidance is provided within the IFtL Artificial Intelligence Policy, which should be read alongside this policy.

8. Data Protection and Information Security

The Trust is committed to protecting personal information and ensuring that all personal data is processed lawfully, fairly and securely.

Effective information security supports safeguarding by protecting the confidentiality, integrity and availability of the information held about pupils, staff and the wider school community.

All members of the Trust community are expected to handle personal information responsibly and in accordance with the Trust's data protection policies and procedures.

Information Security

The Trust will implement appropriate technical and organisational measures to protect information and digital systems from unauthorised access, loss, misuse or disclosure.

This includes:

- secure management of user accounts and access permissions;
- appropriate authentication and password management;
- secure storage and transfer of information;
- appropriate backup and recovery arrangements;
- management of information security incidents;
- regular review of security arrangements and emerging risks.

Staff Responsibilities

Staff are responsible for protecting the information they access as part of their role.

Staff must:

- access personal information only where this is necessary for their role;
- protect confidential information from unauthorised access or disclosure;
- use only Trust-approved systems and services for storing, processing or sharing personal information;
- report actual or suspected data breaches immediately in accordance with Trust procedures;
- comply with the Trust's Data Protection Policy, Information Security procedures and Staff Code of Conduct.

Personal data must not be entered into publicly available or unapproved Artificial Intelligence (AI) tools or online services unless authorised following appropriate data protection assessment and safeguards.

Pupils

Pupils will be taught the importance of protecting their own personal information and respecting the privacy of others as part of the Trust's online safety curriculum.

This includes understanding:

- what personal information is;
- why it should be protected;
- how to manage privacy settings;
- how to recognise requests for personal information;
- when and how to seek help if they are concerned.

Information Sharing

The Trust recognises that effective safeguarding depends upon the timely and appropriate sharing of information where necessary to protect children.

Information will be shared lawfully, proportionately and in accordance with safeguarding legislation, data protection legislation and relevant statutory guidance.

Concerns about a child's safety will never be withheld because of uncertainty about data protection requirements.

Further guidance is available within the Trust's **General Data Protection Policy**, **Information Security procedures** and **Child Protection and Safeguarding Policy**.

9. Digital Communications, Social Media and Online Publishing

The Trust recognises that digital communication is an essential part of education, safeguarding and school life. Staff, pupils and the wider school community use a range of digital platforms to communicate, collaborate and celebrate learning.

The Trust is committed to ensuring that all online communication is safe, appropriate, professional and compliant with safeguarding, data protection and copyright requirements.

Professional Conduct

Staff are expected to maintain appropriate professional boundaries at all times when communicating online.

Staff must:

- use only Trust-approved communication platforms when communicating with pupils or parents/carers;
- ensure that all electronic communication is professional, appropriate and consistent with their role;
- not communicate with pupils through personal social media accounts or private messaging services;
- follow the Staff Code of Conduct and Acceptable Use Policy when using digital technologies;

- report any inappropriate online communication or safeguarding concerns immediately.

School Websites and Online Publishing

The Trust uses websites and digital platforms to communicate with parents, carers and the wider community and to celebrate pupils' achievements.

Published content will:

- support the educational aims and values of the Trust;
- be accurate, appropriate and regularly reviewed;
- comply with safeguarding, copyright and data protection requirements;
- avoid publishing unnecessary personal information.

Pupil images, names and other personal information will only be published in accordance with the Trust's consent procedures and data protection requirements.

Particular consideration will be given to reducing the risk of images being copied, manipulated or misused, including through Artificial Intelligence (AI) technologies.

Social Media

The Trust recognises that social media can provide valuable opportunities for communication, education and community engagement. Staff should be aware that personal online activity may impact on professional responsibilities where it creates safeguarding concerns or undermines trust and confidence in their role.

Staff, pupils and visitors are expected to use social media responsibly and in a manner that does not place themselves or others at risk.

Staff must not:

- identify or discuss individual pupils or families on personal social media accounts;
- share photographs or videos of pupils using personal devices or accounts;
- publish confidential or sensitive Trust information;
- make comments that could undermine professional standards or bring the Trust into disrepute.

The Trust may take action where online behaviour, whether occurring on or off Trust premises, poses a safeguarding risk or has a significant impact on members of the Trust community.

The Trust recognises that concerns, complaints or allegations may be raised by parents, carers or members of the public through digital platforms, including social media. Such matters will be managed in accordance with the appropriate safeguarding, complaints, staff conduct or other relevant procedures, as applicable.

Email and Digital Communication

Trust email systems are provided primarily for educational and professional purposes.

Staff and pupils must:

- use Trust-provided accounts where appropriate;
- remain vigilant to phishing attempts, scams and malicious communications;
- report suspicious emails or messages to the IFtL IT Team;
- avoid opening attachments or following links from unknown or untrusted sources.

Copyright and Intellectual Property

All members of the Trust community must respect copyright, licensing arrangements and intellectual property rights when creating, sharing or using digital content.

Pupils will be taught to acknowledge sources appropriately and understand the importance of academic honesty, including when using Artificial Intelligence (AI) tools.

10. Mobile Phones and Personal Devices

The Trust recognises that mobile phones, smart devices and other personal technologies form part of everyday life. Whilst these devices offer significant educational and communication benefits, they can also present safeguarding, wellbeing, privacy and cyber security risks.

Each IFtL school will have clear procedures governing the use of mobile phones, smart technology and other personal devices that reflect the age of pupils, the context of the school and current Department for Education guidance.

Schools will consider Department for Education guidance relating to mobile phones and behaviour expectations when developing local procedures.

Pupils

Pupil use of mobile phones and personal smart devices during the school day will be managed in accordance with each school's Behaviour Policy and local procedures.

Where pupils are permitted to bring personal devices onto the school site:

- devices must be stored securely when not authorised for use;
- devices must not be used in a manner that compromises safeguarding, learning or the wellbeing of others;
- pupils must not use personal devices to photograph, film or record other individuals without permission;
- pupils must not use personal devices to access or distribute inappropriate, harmful or illegal material;
- pupils must comply with staff instructions regarding the use or storage of personal devices.

The use of mobile data or alternative internet connections to bypass the Trust's filtering and monitoring systems is prohibited whilst on school premises.

Staff

Staff may use personal devices in accordance with the Staff Code of Conduct and school procedures.

Staff must not:

- use personal devices to communicate with pupils;
- photograph or record pupils using personal devices except where expressly authorised in exceptional circumstances;
- store personal or confidential Trust information on personal devices unless authorised and appropriately secured.

Staff are expected to model safe, responsible and professional use of technology at all times.

Visitors

Visitors, contractors and volunteers using personal devices whilst on Trust premises must comply with safeguarding procedures and any instructions provided by the school.

School Devices

The Trust provides digital devices and systems to support teaching, learning and school operations.

Users of Trust-owned devices are expected to:

- use devices safely, responsibly and for their intended purpose;
- protect devices from damage, loss or theft;
- report faults, loss, theft or security concerns promptly;
- comply with the Trust's Acceptable Use Policy and information security requirements.

Trust-owned devices remain subject to the Trust's filtering, monitoring and cyber security arrangements whether used on or off site.

11. Remote Learning and Online Platforms

The Trust recognises that online platforms and digital technologies are an integral part of teaching, learning and communication. Whether learning takes place on site or remotely, safeguarding expectations remain the same.

All online learning activities must support a safe, inclusive and effective learning environment and be delivered using Trust-approved platforms and digital services.

Safe Use of Online Platforms

The Trust will ensure that:

- only approved digital platforms and applications are used for teaching, learning and communication with pupils;
- access to online learning platforms is appropriately managed and secured;
- appropriate filtering, monitoring and cyber security arrangements remain in place where applicable;

- pupils are taught how to participate safely and responsibly in online learning environments.

Staff Responsibilities

When delivering learning online, staff will:

- maintain the same professional standards and safeguarding expectations that apply within the classroom;
- communicate with pupils only through Trust-approved systems;
- use school accounts and devices wherever possible;
- follow the Staff Code of Conduct and safeguarding procedures at all times;
- report any safeguarding concerns arising during online learning immediately to the Designated Safeguarding Lead (DSL).

Learner Responsibilities

Pupils are expected to:

- engage with online learning respectfully and responsibly;
- follow the expectations set out in the Acceptable Use Agreement;
- report anything online that makes them feel worried, unsafe or uncomfortable;
- respect the privacy, dignity and rights of others when participating in online activities.

Parents and Carers

Parents and carers play an important role in supporting safe online learning.

The Trust will provide information, guidance and support to help families understand:

- the digital platforms used by the school;
- expectations for safe and appropriate online behaviour;
- how to report concerns relating to online safety;
- where to access further advice and support.

12. Training and Continuous Professional Development (CPD)

The Trust recognises that effective online safety depends upon knowledgeable, confident and well-supported staff. Online safety is therefore embedded within the Trust's wider safeguarding culture and professional development programme.

All staff, governors, trustees and volunteers will receive appropriate information and training proportionate to their role.

Training will be proportionate to individuals' roles and responsibilities and will be reviewed regularly to reflect emerging technologies, safeguarding risks and changes to statutory guidance.

Staff Training

All staff will receive training which enables them to:

- understand their safeguarding responsibilities in relation to online safety;
- recognise, respond to and report online safety concerns;
- understand the Trust's expectations for filtering and monitoring and their role within these arrangements;
- promote safe, responsible and appropriate use of technology;
- understand the opportunities, limitations and safeguarding implications of Artificial Intelligence (AI);
- protect personal information and recognise cyber security risks, including phishing, social engineering and data breaches;
- understand professional conduct and appropriate use of digital technologies.

Online safety updates will be provided throughout the year through safeguarding briefings, professional development activities and other communications where appropriate.

Designated Safeguarding Leads

The Designated Safeguarding Lead (DSL) and Deputy DSLs will undertake appropriate safeguarding and online safety training to enable them to:

- fulfil their statutory safeguarding responsibilities;
- understand filtering and monitoring systems and processes;
- identify and respond to emerging online harms;
- support staff and pupils effectively;
- work collaboratively with the IFtL IT Team and external partners where appropriate.

IFtL IT Team

Members of the IFtL IT Team will undertake appropriate professional development to ensure they maintain current knowledge of:

- cyber security;
- filtering and monitoring technologies;
- information security;
- emerging technologies;
- relevant statutory guidance and recognised good practice.

The IFtL IT Team will work collaboratively with school leaders and DSLs to support the effective implementation of this policy.

Governors and Trustees

Governors and Trustees will receive safeguarding training at induction and regular updates thereafter, including:

- their strategic responsibilities for online safety;

- the requirements of Keeping Children Safe in Education;
- filtering and monitoring standards;
- cyber security awareness;
- providing effective challenge and oversight of safeguarding arrangements.

Pupils

Online safety education is delivered through a planned and progressive curriculum which is appropriate to pupils' age, stage of development and individual needs.

Learning is reinforced through assemblies, pastoral activities, curriculum opportunities, national awareness campaigns and wider safeguarding education.

Parents and Carers

The Trust will support parents and carers by providing information and guidance to help them understand online risks and promote safe use of technology at home.

Information may be shared through newsletters, workshops, the Trust and school websites, online resources and other appropriate communication channels.

13. Monitoring, Review and Evaluation

The Trust recognises that online safety is an evolving area, with new technologies, platforms and risks developing continuously. Effective online safety arrangements require regular monitoring, evaluation and review to ensure that practice remains effective, proportionate and responsive to emerging risks.

The implementation and effectiveness of this Online Safety Policy will be monitored through a combination of safeguarding oversight, technical assurance, education review and stakeholder feedback.

Monitoring Arrangements

The Trust and its schools will monitor online safety arrangements through:

- review of online safety incidents, including themes, patterns and outcomes;
- analysis of filtering and monitoring alerts and reports;
- review of safeguarding records relating to online harms;
- feedback from pupils, staff, parents and carers;
- review of online safety education and curriculum delivery;
- evaluation of staff confidence and training needs;
- technical reviews undertaken by the IFtL IT Team.

Monitoring information will be used to identify trends, emerging risks and areas for improvement.

Filtering and Monitoring Review

In accordance with [Department for Education Filtering and Monitoring Standards](#) and [Keeping Children Safe in Education](#), the effectiveness of filtering and monitoring

arrangements will be reviewed regularly through operational checks, safeguarding review and governance oversight.

The review will include consideration of:

- whether filtering systems are working effectively;
- whether monitoring arrangements identify relevant safeguarding concerns;
- whether systems are appropriately balanced to protect pupils whilst enabling effective teaching and learning;
- whether staff understand their roles and responsibilities;
- whether any improvements or changes are required.

The review will involve appropriate representatives, including:

- senior leaders;
- the Designated Safeguarding Lead (DSL);
- the IFtL IT Team;
- governors/trustees where appropriate.

Records of filtering and monitoring checks, reviews and actions will be maintained by the Trust.

Governance and Assurance

Governors and Trustees provide strategic oversight and challenge to ensure online safety arrangements remain effective.

Safeguarding reports will provide appropriate assurance regarding:

- online safety incidents and emerging themes;
- filtering and monitoring effectiveness;
- staff training completion;
- curriculum provision;
- actions arising from audits and reviews.

Information shared with governors and trustees will be anonymised and proportionate, ensuring confidentiality is maintained.

Policy Review

This Online Safety Policy will be reviewed:

- annually;
- following significant changes to statutory guidance;
- following significant technological developments;
- following significant incidents or learning from practice.

Reviews will consider:

- changes in online risks and technology;
- national guidance and statutory requirements;
- feedback from pupils, staff and parents/carers;
- safeguarding and technical incident trends;
- recommendations from audits or external reviews.

The policy will be approved through the Trust's governance arrangements and communicated to the wider school community.

14. Linked Policies, Procedures and Guidance

This Online Safety Policy should be read alongside the following Trust and school policies, procedures and guidance:

Trust Policies

[IFtL Child Protection and Safeguarding Policy](#)

[IFtL Behaviour Policy](#)

[IFtL Anti-Bullying Policy](#)

[IFtL Staff Code of Conduct](#)

IFtL Acceptable Use Policy / Agreements

IFtL Artificial Intelligence (AI) in Education Policy

[IFtL Data Protection Policy](#)

IFtL Cyber Security Policy

[IFtL Social Media Policy](#)

[IFtL Complaints Policy](#)

[IFtL Whistleblowing Policy](#)

[IFtL Equality, Diversity and Inclusion Policy](#)

School-Level Documents

Where applicable, this policy should also be read alongside individual school procedures relating to:

- mobile phones and personal devices;
- behaviour expectations;
- remote learning and online platforms;
- digital communication and publishing;
- pupil acceptable use agreements;
- parent/carers agreements relating to digital technology and devices.