Inspiring Futures through Learning

Online Safety Policy

September 2025 to September 2026

Policy name:	IFtL Online Safety Policy
Version:	V2
Date relevant from:	September 2025
Date to be reviewed:	September 2026 *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.*
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:	28 August 2025

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 from 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.*

Philosophy

At our IFtL schools, the development of all children's social, moral, spiritual, and cultural growth is paramount. We believe that the most important function of the school is to maintain an environment in which every member of the school can achieve success and self-fulfilment.

There must be a total consistency of expectation that everyone (irrespective of protected characteristics) should feel safe and secure, have empathy for all others, and place a high value upon individual achievement and personal development.

Over the last few years, schools have become increasingly reliant on IT systems and infrastructure to deliver critical services. At the same time, the threat from criminals and other bad actors has increased exponentially.

This policy aims to set minimum standards for schools with the aim of ensuring that their systems are as protected as they can be against the threat of ransomware, malware, and cyber-attack. Some of the language in this document may be technical but we have tried to keep it as understandable as possible.

Safeguarding

At our IFtL schools, Child Protection and Safeguarding is paramount and we are fully committed to ensuring the welfare and safety of all our children. Our effective approach to online safety empowers our schools to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Students have a right to learn in a supportive, caring, and safe environment which includes the right to protection from all types of abuse, where staff are vigilant for signs of any student in distress and are confident about applying the processes to avert and alleviate any such problems. If any behaviour is a concern inrelation to safeguarding; procedures and processes will be always followed in accordance with the Child Protection and Safeguarding Policy. Any concerns will be referred to the Designated Safeguarding Lead, or the Deputy Designated Safeguarding Leads.

IT Health, Safety and Welfare

The internet is becoming as commonplace as the telephone or TV today; its effective use is an essential element in 21st Century life for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. IFtL has a duty to provide students with quality internet access as part of their learning experience.

Online safety includes, but is not limited to, browsing the internet. Other forms of electronic communication and interaction such as e-mail, blogging, social networking, online gaming

and Artificial Intelligence should be considered as well as the corruption, misuse, hacking, and publication of personal data.

When using the internet, children and young people must be safeguarded from a range of online risks, including exposure to violence, racism, exploitation, and the potential misuse of emerging technologies such as artificial intelligence (AI) tools. While the internet hosts a wide range of content, not all of it is age appropriate. Pupils may come across material that is unsuitable or harmful, including content intended for adults or that promotes unsafe behaviour. They need to learn to recognise and avoid any potential risks – to become "Internet Wise". Pupils need clear guidance to prepare them to respond appropriately to any situation, using any of the previously mentioned methods of electronic communication, for the inevitable moment when they come across inappropriate material or find themselves in an uncomfortable situation. Online safety is explicitly taught within the PSHE and safeguarding curriculums.

The purpose of this policy is to help ensure the online safety of all pupils and staff. It supports our responsibility to provide a safe digital environment and to educate pupils on recognising online risks and responding to them safely and responsibly.

Writing, agreement and review of the Online Safety Policy

Our online Safety Policy has been written using Local Authority and Government advice. It has been agreed by the Executive Board and Trustees. The policy and its implementation will be reviewed annually.

Why the Internet and electronic communication use is important

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet use forms part of the statutory curriculum and as such is a necessary tool for learning.

The Internet forms part of everyday society and as such it is every schools' duty to prepare its pupils through quality Internet access with the personal tools to evaluate information and to take care.

There are benefits to the Internet and planned Government initiatives such as:

- Access to world-wide educational resources. (Museums or Galleries)
- Inclusion in the National Education Network connecting schools together.
- The potential for world-wide educational materials and resources to enhance the National Curriculum.
- Exchange of curriculum and assessment data between National Bodies
- Access school assessment, curriculum and personal resources from any location that has an internet connection.
- The facility to extend learning beyond the traditional school building into a contemporary digital environment

How the internet will be used to enhance learning:

- School Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- All classes will be taught the school's 'Rules for Responsible Internet Use' at the start of each school year, alongside the skills needed to use the internet safely and appropriately. Pupils in all year groups will be supported to understand these expectations and will be asked to agree to use the internet responsibly, as taught. Headteachers will monitor implementation across the school.
- Internet access will be planned to enrich and enhance learning activities, and pupils will begiven clear objectives for all Internet use.
- Pupils will be educated in the effective use of Internet in research, including the skills ofknowledge location and retrieval.
- Supervision is the key strategy - aimless surfing should never be allowed. Pupils shouldalways use the Internet in response to an articulated need.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the to the IT Help Desk via the DSL.
- Schools should ensure that the use of the Internet derived materials by staff and pupilscomplies with copyright law.
- Pupils will be taught to acknowledge the source of information and to respect copyrightwhen using information from the Internet.
- Pupils are encouraged to approach online content — including AI-generated material — with critical thinking and appropriate caution, understanding that not all information is accurate, safe, or trustworthy.

Security of information and systems

Online safety will encompass the security of not only the Internet but the delivery of Internet services and computer applications in school. Issues surrounding the security of access are deemedas important as safeguarding staff and pupils use on on-line activities.

Staff and pupils will be expected to take responsibility for their use of the network. As part of theirdaily use, they can be reasonably expected to:

- Keep their password secret from peers.
- Ensure that they securely logoff from any iPad/workstation they use during the day.
- Clean up unused files from the devices/network to assist with the longevity of disk storage devices.
- Portable storage devices or media (e.g. USB drives) are not permitted. Staff must not use or connect such devices to school systems.
- Password protect any confidential or sensitive information.
- Not open any attachments, executables, or files from unknown or untrusted sources.
- Report any concerns or possible breaches of security to the Data Protection Officer in school.
- Realise the school IT systems are not for personal use.
- Not take copies/download any materials that belong to or are the intellectual property of the school.
- Leave copies of any planning or resources, created using IT, that are required by the school.

The IFtL IT Department will take reasonable steps to ensure:

- Workstations will be configured to prevent user mistakes, deliberate actions or tampering. Servers will be located in a locked room with only key personnel given access to the room.
- Virus protection systems will be provided, secured and kept up to date.
- Access by wireless devices will be strictly controlled and ad-hoc access prevented through the use of authentication protocols.
- The operating systems will be secure and kept up to date.
- All inbound internet connections are configured to prevent unauthorised access.
- On premise firewalls will be in place to prevent unauthorised access.
- Files held on the school network will be periodically scanned for content.
- Monitoring of files and Internet usage will be handled in a professional and discrete way.
- Breaches of protocols will be discussed and acted upon in collaboration with the appropriate people.
- The IFtL IT Manager will review system security and capacity regularly.
- Locally block access to websites or any other content that it deems inappropriate (theblocked list).
- Act upon requests from schools in the event of any inappropriate materials inadvertently being accessed via the Internet that were not alerted by the filtering solution.

Filtering and Monitoring Protection

As per the statutory guidance from the DfE published for September 2025 in the KCSIE, there are 4 C's that this policy must consider and appropriately plan for when filtering and monitoring content students and staff access online:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, **misinformation, disinformation (including fake news) and conspiracy theories**.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non- consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Across our IFtL schools, Lightspeed is our filtering and monitoring safeguarding solution for all registered pupil devices accessing our networks. It provides filtering, monitoring, and alerting functionality that our DSL's are trained in utilising and reporting from. Our leadership

team have an awareness and understanding of the provisions in place and manage them effectively too.

We have consulted the Department for Education's filtering and monitoring standards when designing our provision and, as a result, have:

- Identified and assigned roles and responsibilities to manage filtering and monitoring systems.
- Ensured the review of our filtering and monitoring provision monthly.
- Developed effective monitoring strategies to meet the safeguarding needs of students and staff.
- Blocked harmful and inappropriate content without unreasonably impacting teaching and learning, taking into consideration that 'over blocking' can lead to unreasonable restrictions as what children can be taught with regard to online teaching and learning.
- Schools can use the department's 'plan technology for your school service' to self-assess against the filtering and monitoring standards and receive personalised recommendations on how to meet them.

The services provided by Lightspeed conform to the standards set out by the UK Safer Internet Centre.

All pupil and staff devices must be registered on the network before access to Wi-Fi is granted. This ensures that their online access can be appropriately monitored and filtered.

Web access by pupils is filtered by *Lightspeed* to prohibit access to forbidden material and to provide age-appropriate access to other sites. Web activity is logged automatically, and checks are made of suspicious searches containing, amongst other things, terrorism, sexually abusive and self-abusive language. Records of suspicious searches are reviewed and followed up as appropriate with the pupil who executed the search.

All IFtL schools have an appropriately configured firewall and internet filtering in place to help protect all users — including staff, pupils, and visitors — from inappropriate or harmful content.

All firewall devices have their default username and password changed to a complex password with alerts sent if that password has appeared in any data breach, both inside and outside of the organisation. The details are kept secure and only shared between Trust IT Staff where required.

Personal Data (to be read in conjunction with the IFtL General Data Protection Policy)

Personal data stored about staff, pupils and parents on the school network will only be accessed when needed for work purposes. Members of staff will only have access to this information in an appropriate way. Personal data about any stakeholder must not be entered into generative AI platforms. While some applications include AI-powered features, generative AI tools (e.g. ChatGPT, Copilot) must not be integrated into the workspace or used for processing personal data unless explicitly approved by the IFtL IT department and the IFtL Data Protection Officer (DPO). All AI use must align with the IFtL AI Policy.

Only staff who require access to BromCom or other personal data held by IFtL (either in schools or centrally) as part of their day-to-day role are granted access. Access is strictly limited to those with appropriate authorisation and is regularly reviewed.

Personal data can only be accessed via secure log-on. This ensures that sensitive information cannot be accessed. When a staff member ceases to be employed by IFtL, their accounts are promptly removed by the IT Team upon receiving notification.

E-Mail

Directed e-mail use can bring significant educational benefits. However, the use of e-mail requiresthat appropriate safety measures are also put into place. All schools currently using student email are filtered and subject to monitoring.

- Pupils may only use approved e-mail accounts on the school system.
- Pupil access to external e-mail addresses is not permitted on any IFtL provided device.
- Staff will be encouraged not to access external e-mail accounts at school. Any access duringdirected teaching time is strictly forbidden.
- Pupils must immediately tell a teacher if they receive an offensive or **unfamiliar/suspicious** e-mail.
- Pupils must not reveal details of themselves or others, such as their address or telephonenumber, or arrange to meet anyone through e-mail communication.
- The forwarding of **spam/harmful emails** chain letters is banned.
- Official e-mail sent to parents should be written carefully and authorised before sending.
- Staff should ensure all emails sent are professional and courteous.

The Management and Publication of Content

In this age, the use of websites and social media to showcase a school and the work it produces has become extremely popular. However, it does provide opportunities for acquiring sensitive and personal data if consideration is not given to the material available.

The publication of unique pupil identifiers, images of pupils' faces, or full names is strictly controlled and must only occur with appropriate consent and in line with safeguarding and data protection requirements. These publishedimages could be re-used, especially if a large image has been used. In addition to this, the publication of names and contact details of staff will be kept to a minimum and where necessary.

Only the schools contact details will be published. Staff or pupil contact information will not be published. School leaders will take editorial responsibility and ensure content is accurate and appropriate. At all times, intellectual property and copyright rights will be respected and complied with.

- Under no circumstances is a pupil's full name to be published anywhere on a website,especially when it might relate to a photograph.
- Parents have the right to opt out of any digital publication of their child's images or personal information on the internet. The school will respect this decision in line with

data protection principles, including the lawful basis of 'Public Task' for publishing essential materials.
- The 'opt out' information will be updated annually, and records will be kept.
- At all times, the pupil in photographs should, of course, be appropriately clothed.

Social Networking and Personal Publishing

The recent upsurge in the popularity of social networking sites such as Facebook, Snapchat, Instagram, Twitter and TikTok, many of which already make use of AI and therefore require schools to be aware of the potential dangers and associated risks to staff and pupils. It has become much easier for individuals to publish content and information about themselves on theInternet. The risk of identity theft and the misuse of published photographic material should be considered as risks by all and appropriate steps to educate and protect staff and pupils be made.

- Social networking sites will be blocked on IFtL devices for pupils
- Consideration will be given, at all times, on how to educate pupils in their safe use.
- Pupils will be advised never to give out information that will identify themselves, their friends or their location
- Pupils will be directed towards moderated sites via lightspeed filtering and monitoring
- Pupils will be encouraged not to publish photographic content of themselves.
- Staff should not identify pupils or their place of work in status updates.
- Staff will be advised not to accept requests from current or past pupils.
- Staff must not publish any photographic content featuring pupils or images taken on school premises via their personal social media accounts or other personal platforms. Such actions are deemed inappropriate and breach the school's Code of Conduct and safeguarding policies.
- Staff should not publish status updates regarding school life.

Filtering Internet Content

In a perfect world, filtering would be 100% accurate and inappropriate material would not be visible topupils using the Internet. In practice, this is not easy to achieve and cannot be granted. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable, or threatening. Filtering and monitoring are provided by Lightspeed for all registered student devices.

- The school will ensure systems are in place to filter website content.
- The IFTL IT Manager in conjunction with the school DSL will make checks to ensure that the filtering and monitoring is appropriate, effective andreasonable wherever possible.
- Lightspeed will be used to further control the websites available within the school.
- Lightspeed will be used to temporarily open access to websites for educational use byteaching staff. (All temporary access must be agreed with the IFtL IT Department and strict timings agreed.)
- YouTube and other video content websites will be available in school for the use of

teachersand support staff. Children are permitted to access YouTube or video content websites at school, but only with permission and supervision of a member of teaching staff.

If for any reason, the filtering blocks a website that a class teacher feels would be of benefit to the children then it can be added to a whitelisted category within Lightspeed and therefore be unblocked for teacher/pupiluse. Such requests should be made to the IFtL IT Manager who will decide on whether or not to add the website to the whitelist.

The school will also regularly monitor the websites that children access by using the Lightspeed dashboard. Reports can be produced of the most visited websites; a picture of the usage and activities of the children can be obtained.

The list of websites can be reviewed by schools DSLs, as and when appropriate, additional domains and websites may be added to the blocked list.

Videoconferencing and Webcams

The rapid expansion of communications technology requires the school to have a policy on itspotential use in education.

- All videoconferencing and webcams must only be used by school staff
- Teachers must request permission from SLT before making a call or using a webcam in a lesson with children
- At no point will any live streaming from school be permitted to be viewed outside of school approved applications (i.e. Office 365 teams)

Managing new technologies

Small wireless devices brought into school by pupils provide additional opportunities for accessing online content. These personal devices are not normally connected to the school's Wi-Fi network and therefore cannot be monitored, controlled, or filtered by the school's security systems. Should a device manage to connect to the school Wi-Fi, the on-premises firewall will block access to some inappropriate content, but full control and filtering cannot be guaranteed. This can even extend to games consoles used in after school care clubs where it is possible to connect to global gaming networks and interact with other people – these devices must be always supervised by a staff member. At all times we need to be aware of the current technology and its possible risk and educational benefit.

New technologies such as AI are developing rapidly and due notice should be taken of the Generative artificial intelligence (AI) in education Policy and frequent updates and training on any new AI trends to be shared with IFtL staff where applicable. The Department for Education has published Generative AI: product safety expectations to support schools to use generative artificial intelligence safely, and explains how filtering and monitoring requirements apply to the use of generative AI in education.

- Pupils' mobile phones and other personal smart devices are to be stored securely - such as in a locked tin or cupboard - during the school day, in line with each school's

specific policy and procedures.
- The use of cameras on mobile phones is not permitted.
- A blog may only be used in school by pupils if it is appropriately moderated and required for educational purposes.
- The school will endeavour to ensure its network is as secure as possible to minimise the risk of external attack from outside sources that are not part of the IFtL network. This is achieved by firmware updates to the schools' firewalls.
- The use of mobile data on personal devices is not permitted by students when in school as it will bypass all school filtering systems.

The Prevent Duty and Online Safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe online. Internet safety and safeguarding are integral to our curriculum. Our staff are aware of the risksposed by online activity of extremists and have a duty to act if they believe the wellbeing of any pupil is being compromised.

Protection of Personal Data

Personal data will be recorded, processed, transferred, and made available according to the DataProtection Act (DPA) 1998 and the General Data Protection Regulation (GDPR) 2018.

Authorisation and Supervision of Internet Access

- Pupil internet use is supported by filtering and monitoring systems to help reduce risks. Staff remain responsible for providing appropriate supervision, guidance, and timely support to pupils when using online resources.
- Staff and pupils must be fully aware of the rules and responsibilities regarding IT use before accessing any resources.
- All staff are required to read and sign the 'Staff Code of Conduct'.
- Pupils receive online safety education and agree to a 'Pupil Code of Conduct'. Families also consent to terms such as the iPad Home School Agreement and Digital Technology Acceptable Use Policy as part of the Futures Focused project.
- A current record of all users granted access to the school network is maintained.
- Visitors or contractors must be informed of acceptable IT use before accessing school systems.

Risk Management

- The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the vast and interconnected nature of internet content, it cannot guarantee that unsuitable material will never be encountered on IFtL devices and is not liable for any consequences arising from internet use.

- Online safety policies and their implementation are regularly audited to ensure effectiveness.
- DSLs frequently monitor Lightspeed data, reviewing search terms and alerts, and report significant findings weekly to the Head of Safeguarding. This information is discussed with the Head of IT and IFtL Education team to review and adjust filtering settings or school practices as necessary.

Online Safety complaints

- Staff misuse will be referred to the Head of School.
- Complaints made about Internet misuse will be dealt with by the school in the first instance.
- Complaints of a child protection nature must be dealt with in line with the school Child Protection Procedures.
- Parents and pupils will be informed of any necessary complaints' procedure – refer to complaints policy.
- Parents, pupils and staff will be made aware of the consequences of the misuse of the Internet or any IFtL resources. This can be found in the Future Focused project documentation for IFtL use.

Regulation and Conduct

- The use of internet and email, as valuable but potentially misused resources, must be regulated through clear, fair rules prominently displayed near all computer systems.
- Pupils will be informed that their internet and email use is monitored and will receive instruction in responsible and safe usage before access is granted.
- Staff responsibilities regarding online safety are communicated via the online safety policy, which includes awareness that internet use may be monitored.
- Monitoring is overseen by the DSL, who follows established procedures for reporting concerns.
- Parents and carers are made aware of the school's online safety policies, which are accessible on the IFtL website.

Abuse of the System

Any transgressions of the rules which are minor can be dealt with by the teacher as part of normalclass discipline. Other situations could potentially be serious and sanctions available include:

- An interview/counselling by a member of SLT
- Informing parents or carers
- The removal of Internet or computer access for a set period of time

CPD linked to this policy

Training for staff is undertaken annually, now in I A compliant, formerly SmartLog. In school training also takes place and online safety forms part of the regular Safeguarding briefings in schools. CPD includes delegates understanding the online safety expectations and applicable roles and responsibilities in relation to filtering and monitoring.

Training is provided as part of induction processes, and this is for both staff and governors / trustees.

Other policies/documents to be considered alongside this one:

- IFtL Child Protection and Safeguarding Policy
- IFtL Using Artificial Intelligence in Education Policy
- IFtL Code of Conduct for Staff
- IFtL Complaints Procedure
- IFtL Acceptable use policy for staff
- Home School agreement
- Terms and conditions for iPad use
- IFtL General Data Protection Policy
- Suite of Future Focused documents