Inspiring Futures through Learning

# Online Safety Policy

September 2023 to September 2025

| | |
|---|---|
| **Policy name:** | IFtL Online Safety Policy |
| **Version:** | V1 |
| **Date relevant from:** | September 2023 |
| **Date to be reviewed:** | September 2025<br>*This policy will be reviewed every two years 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. |
| **Statutory (Y/N):** | Y |
| **Published on website*:** | 1B |

| | |
|---|---|
| **Policy level**:** | 1 |
| **Relevant to:** | All employees through all IFtL schools and departments |
| **Bodies consulted:** | Employees<br>Trade unions<br>School / department governance bodies |
| **Approved by:** | IFtL Board of Trustees |
| **Approval date:** | 29th August 2023 |

**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.
     - o *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.
     - o *Approved by the IFtL Board of Trustees as a Trust Core Values policy.*
     - o *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
     - o *Approved by school / department governance bodies.*

**Philosophy**

At **Rickley Park School**, 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 is able to achieve success and self-fulfilment.

There must be a total consistency of expectation that everyone (irrespective of gender, race, orculture) 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 more and more reliant in 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 **Rickley Park School**, Child Protection and Safeguarding is paramount and we are fully committed to ensuring the welfare and safety of all our children. 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 concernin relation to Safeguarding, procedures and processes will be followed at all times 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.

**Commented [BS1]:** Rater than name here, how about a block on Page 1 with the relevant people and contacts listed. That makes it easier to maintain.

**Commented [BS2R1]:** Also include
ICT Lead
Online Safety Lead
Trust IT Contact email/tel

**ICT Health, Safety and Welfare**

The internet is becoming as commonplace as the telephone or TV in today's society; its effective useisan 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. Our school 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, and online gaming should be considered as well as the corruption, misuse, hacking, and publication of personal data.

When using the internet, young people need to be protected from dangers including violence, racism, and exploitation. Much of the material on the internet is published for an adult audience andtherefore may be unsuitable for pupils.  They need to learn to recognise and avoid any potential risks – to become "Internet Wise". Pupils need clear guidance in order 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.

A clear school policy is required to help to ensure the safety of our staff and pupils. We have a requirement to provide pupils with as safe an environment as possible and a need to teach them tobe aware of and how to respond responsibly to any of the risks.

Writing, agreement and review of the Online Safety Policy

Our online Safety Policy has been written by the school using Local Authority and Government advice. It has been agreed by the SLT 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 thathas an internet connection.
- The facility to extend learning beyond the traditional school building into an electronic environment

How the internet will be used to enhance learning:

- School Internet access will be designed expressly for pupil use and will include filteringappropriate to the age of pupils.
- All classes will be taught 'Rules for Responsible Internet Use', at the beginning of a school year, and the skills needed in order to use the Internet appropriately. Children in all classeswill sign an agreement to use the internet appropriately and responsibly, as they have beentaught to.
- 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 Internet Service Provider via the Online Safety Lead.
- 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.

**Commented [BS3]:** Should this be to the DSL as well to then report to IT or Direct to IT. I'm not sure Schools would go directly to the ISP?
If something has been accessed then it has been seen. Unless accessed by mistake it has been deliberately searched for.

### 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 workstation they use during the day.
- Clean up unused files from the network to assist with the longevity of disk storage devices.
- Ensure the removal and secure storage of any portable storage devices or media.
- 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 ICT Lead.
- Realise the school ICT space is not personal space.
- Not take copies of any materials that belong to or are the intellectual property of the school.
- To leave copies of any planning or resources, created using ICT, that are required by theschool.

**Commented [BS4]:** I might go stronger on this and suggest that portable storage devices are NOT used anywhere on the IFTL network.

**Commented [BS5]:** Just a suggestion

The Online Safety Lead and Service Provider will take reasonable steps to ensure:

**Commented [BS6]:** Who is this?

- 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 throughthe use of authentication protocols.
- The server operating system will be secure and kept up to date.
- All inbound internet connections are configured to prevent unauthorised access.
- Firewalls will be in place to prevent unauthorised access.
- Files held on the school network will be regularly checked for content.

**Commented [BS7]:** A note or two is needed about Visitor, Guest, Governor access.

**Commented [BS8]:** If this is the case, what is the procedure for doing this and how/where is it logged?

- 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 Online SafetyLead and SLT.
- The Online Safety Lead will review system security and capacity regularly.
- Locally block access to websites or any other content that it deems inappropriate (theblocked list).
- Notify the IFtL Trust IT Manager in the event of any inappropriate  materials inadvertently being accessed via the Internet that were not alerted by the filtering solution.

**Commented [BS9]:** What is the Online Safety Leads training and capacity needs around this - not a policy thing, but security reviews can be extensive and it would be good to get some clarification on how and when this is checked for Cyber Security audit purposes

**Firewalls and Perimeter Protection**

As per the statutory guidance from the DfE published for September 2023, 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, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

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

**conduct:** 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.

At **Rickley Park School**, Lightspeed is our safeguarding solution for all registered 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.

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

Commented [BS10]: These could link out to those documents

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 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 or member of staff who executed the search.

In addition, **Rickley Park School** has an appropriately configured firewall between our network and the internet.

All firewall and gateway 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.

Only necessary staff, such as the ICT Technicians, have access to BromCom’s and other personal data that is held by the office.

Personal data can only be accessed via secure log-on and from a managed network. This ensures that sensitive information cannot be accessed when not linked to a school network. “Zombie” accounts (accounts of staff who are no longer employed by the school,) are removed by the ICT Technician when a member of staff is no longer an employee.

**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 school provided e-mail accounts 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.
- 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 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.
- Whole class or group e-mail addresses should be used when classes wish to contact

Commented [BS11]: Can they access their school email on their iPad from home?

external organisations or personnel.

- The forwarding of chain letters is banned.
- Official e-mail sent to parents should be written carefully and authorised before sending.
- Staff should ensure all emails sent to professional organisations are professional andcourteous.

**Commented [BS12]:** banned or strictly forbidden ?

### The Management and Publication of Content

In this age, the use of websites 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.

Unlike newspapers, the publication of pupil faces and full names is not acceptable. 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 discouraged and where necessary, access tothis information will be available via other methods or through a secure portal.

Only the schools contact details will be published. Staff or pupil contact information will not be published. The Online Safety Lead and SLT will take editorial responsibility and ensure content is accurateand 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 will be given the right to 'opt out' of digital publication in any form of their child on the internet.
- 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

**Commented [BS13]:** This section needs something on publishing personal content outside of school on what may be considered a private/personal account.
Worth talking to HR on this.

Also how does this apply to Governors and their roles in the school and externally?

The recent upsurge in the popularity of social networking sites such as Facebook, Snapchat, Instagram, Twitter and TikTok requires schools to be aware of the potential dangers 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.

- All social networking sites will be blocked in school.
- 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.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

**Commented [BS14]:** Really?

It's hard to do the next thing if that is the case.

**Commented [BS15R14]:** What about WhatsApp?

- Pupils will be encouraged not to publish photographic content of themselves.
- Staff should not identify pupils of their place of work in status updates.
- Staff will be advised not to accept requests from current or past pupils.
- Staff must not publish photographic content that contains any images from school or ofpupils.
- Staff should not publish status updates regarding school life.

**Commented [BS16]:** Is it ok to publish status updates regarding home life?

**Filtering Internet Content**

In a perfect world, filtering would be 100% accurate and inappropriate material would not be visible to pupils 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.  Such a procedure will be detailed further into the policy.

- The school will ensure systems are in place to filter website content.
- The Online Safety Lead will make checks to ensure that the filtering is appropriate, effective andreasonable and this is monitored regularly.

**Commented [BS17]:** Whats regular? I'd suggest a set time here like Termly, also how is this logged and verified.

- A local school list will be maintained to further control the websites available within theschool.
- A local school list will be used to temporarily open access to websites for educational use byteaching staff. (All temporary access must be agreed with the technician 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 be a member of teaching staff.

**Commented [BS18]:** Is YT blocked when iPads are used off the school network?

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 and therefore be unblocked for teacher/pupiluse.  Such additions should be made to the Online Safety Lead who will make a decision on whether or not to add the website to the whitelist.

The school will also regularly monitor the websites that children access by using our filtering systems 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 DSL's, 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 make use of the school network to ensure qualityof service and security.
- Teachers must request permission from SLT before making a call or using a webcam

in alesson.

- All webcam use will be supervised.
- At no point will any live streaming from school be permitted to be viewed on the Internet orthrough the school website.

**Managing new technologies**

Small wireless devices provide more opportunities for pupils to be exposed to content within school that cannot be controlled or filtered through the school network or security systems. This can evenextend to games consoles used in after school care clubs where it is possible to connect to global gaming networks and interact with other people. At all times we need to be aware of the current technology and its possible risk and educational benefit.

- Pupils' mobile phones will be stored in a locked tin or cupboard throughout the day.
- 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.
- The school will ensure its network will block connections from devices that are not part of itsdomain. (Personal laptops, iPads, iPod touches, wireless mobiles)
- The use of 3G broadband devices is not permitted 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 is integral to our computing curriculum. Our staff are aware of the risksposed by online activity of extremists and have a duty to take action 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 of Internet Access**

Staff need to be vigilant and ensure that any use of the Internet by pupils must be authorised and supervised at all times. This will ensure that any potential risks are reduced and that a pupil will have an immediate point of contact should they have a problem or are uncertain of action to take. All staff and pupils must be made aware of the rules and regulations surrounding the use of any ICTresource before beginning to use it in education.

- All staff will ensure that they have read and signed a 'Staff Code of Conduct for ICT'.
- All pupils will be taught about online safety and will sign a 'class agreement'.
- At all times a record of staff and pupils who are granted access to the school network will bemaintained.

- Any person not employed by the school must be made aware of the rules and acceptableuse of ICT systems before being allowed access.

**Risk Management**

At all times staff, pupils and parents should be made aware that:

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible toguarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

Regular audits of ICT use will establish if the Online Safety policy is adequate, and that the implementationof the policy is appropriate and effective.

**Commented [BS19]:** Better to set a named frequency and mention how these are logged/referenced

**Online Safety complaints**

- Staff misuse will be referred to the Head of School.
- Complaints made about Internet misuse will be dealt with by the Online Safety Lead and SLT.
- Complaints of a child protection nature must be dealt with in line with the school ChildProtection Procedures.
- Parents and pupils will be informed of any necessary complaints procedure.
- Parents, pupils and staff will be made aware of the consequences of the misuse of theInternet or school resources.

**Regulation**

The use of a limited and expensive resource, which brings with it the possibility of misuse, must be regulated. Fair rules, prominently displayed, will help pupils to make responsible decisions.

- Rules of Internet access and E-mail use will be posted near all computer systems.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede all Internet and E-mail access.
- Staff will be made aware of their responsibilities through the distribution of the online safetypolicy.
- Staff will be informed that Internet use can be monitored.
- Monitoring will be carried out by the Online Safety Lead working to clear procedures for reportingissues.
- Parents/carers will be made aware of the School's online safety policies.

**Commented [BS20]:** Add in process for visitors/governors

**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