Acceptable Use of ICT Policy

Approved by Trust Board:	Approved on 03.09.2026
Policy Owner:	Director of Safeguarding and School Operations (Trust DSL)
Policy Reviewed by:	Executive Team
Version:	4
Next Review:	September 2027
Review Frequency:	Annually
Consultation with Unions:	No
Location of Policy:	Trust Website / Staff SharePoint / Individual School Websites which includes on page 13 the named person for the responsibility in managing our filtering and monitoring systems

This policy is prescribed by Inspire Learning Partnership. All references to 'the Trust', includes all Trust schools and subsidiary organisations. Procurement and funding of ICT is the responsibility of the Director of Finance, working in conjunction with the IT provider.

Inspire Learning Partnership is a charitable company limited by guarantee registered in England and Wales with company number 9202445

Table of Contents

1. Introduction and aims 3
2. Relevant legislation and guidance 4
3. Definitions 4
4. Unacceptable use 5
   4.1 Exceptions from unacceptable use 6
   4.2 Sanctions 7
5. Staff (including those involved in governance, volunteers, and contractors) 7
   5.1 Access to school ICT facilities and materials 7
      5.1.1 Use of phones and email 8
   5.2 Personal use 9
      5.2.1 Personal Devices 10
      5.2.2 Personal social media accounts 11
   5.3 Remote access 11
   5.4 School social media accounts 11
   5.5 Monitoring and filtering of the school network and use of ICT facilities 11
6. Pupils 14
   6.1 Access to ICT facilities 14
   6.2 Search and deletion 14
   6.3 Unacceptable use of ICT and the internet outside of school 16
7. Parents/carers 17
   7.1 Access to ICT facilities and materials 17
   7.2 Communicating with or about the school online 17
   7.3 Communicating with parents/carers about pupil activity 17
8. Data security, including energy consumption 17
9. Protection from cyber attacks 20
10. Internet access 20
   10.1 Pupils 21
   10.2 Parents/carers and visitors 21
11. Monitoring and review 21
12. Related policies 21
13. Appendix 1: Facebook cheat sheet for staff 23
14. Appendix 2: Acceptable use of the internet: agreement for parents and carers 25
15. Appendix 3: Acceptable use agreement for older pupils 26
16. Appendix 4: Acceptable use agreement for younger pupils 28
17. Appendix 5: Acceptable use agreement for staff, those involved in governance, volunteers and visitors 30

Appendix 6: Glossary of cyber security terminology 31

18. Appendix 7 Data Protection Impact Assessment (DPIA) enquiry form 33

Inspire Learning Partnership is a charitable company limited by guarantee registered in England and Wales with company number 9202445

19. Appendix 8: Subscriptions, Contract, SLA enquiry form 34

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our Trust and schools work, and is a critical resource for pupils, staff, those involved in governance, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our Trust uses could also pose risks to data protection, online safety and safeguarding. The Trust recognises online safety risks within the four key areas identified by KCSiE:

- Content: exposure to harmful, inappropriate or illegal content
- Contact: harmful interactions online
- Conduct: behaviour that causes harm online
- Commerce: online scams, phishing, gambling and financial exploitation

Online safety considerations are embedded throughout the curriculum, safeguarding procedures and ICT provision.

The Trust recognises that generative AI systems may expose pupils to safeguarding risks including:

- harmful or inappropriate content
- misinformation and disinformation
- grooming and manipulation risks
- data privacy concerns
- AI-generated nude or semi-nude imagery (deepfakes)
- cyber security threats

The use of AI tools by pupils will be age-appropriate, risk assessed and supervised where required. Staff must only use approved AI applications in accordance with Trust guidance and data protection requirements.

This policy aims to:

- Set guidelines and rules on the use of Trust ICT resources for staff, pupils, parents/carers and those involved in governance
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the Trust's policies on data protection and school's policies on online safety and child protection and safeguarding

Inspire Learning Partnership is a charitable company limited by guarantee registered in England and Wales with company number 9202445

- Prevent disruption that could occur to the Trust or an individual school, through the misuse, or attempted misuse, of ICT systems
- Support schools in teaching pupils safe and effective internet and ICT use

This policy covers all users of our Trust's ICT facilities, including those involved in governance, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our staff disciplinary policy, allegations of abuse against adults' policy, staff code of conduct or behaviour policy.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2026
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people 2024
- Generative AI: product safety expectations 2026
- Meeting digital and technology standards in schools and colleges 2026

3. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web

applications or services, and any device system or service that may become available in the future which is provided as part of the Trust's ICT service

- **Users:** anyone authorised by the Trust to use the ICT facilities, including those involved in governance, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See Appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the Trust's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the Trust's ICT facilities includes:

- Using the Trust's ICT facilities to breach intellectual property rights or copyright
- Using the Trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the Trust, or risks bringing the Trust into disrepute
- Sharing confidential information about the Trust, its pupils, or other members of the Trust's community
- Connecting any device to the Trust's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the Trust's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the Trust's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel

- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the Trust's ICT facilities
- Causing intentional damage to the Trust's ICT facilities
- Removing, deleting or disposing of the Trust's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the Trust
- Using websites or mechanisms to bypass the Trust's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools, wearables and generative chatbots (such as ChatGPT and Google Gemini):
    - During assessments, including internal and external assessments, and coursework
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work
    - To make unauthorised recordings

This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The CEO/Headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Trust's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of the Trust's ICT facilities (on Trust premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the CEO/Headteacher's discretion. Permission should be granted from the CEO/Headteacher before the use, unless it is an emergency or exceptional situation.

Exceptions to the use of artificial intelligence (AI) tools includes:

- Pupils may use AI tools and generative chatbots:
    - As a research tool to help them find out about new topics and ideas
    - When specifically studying and discussing AI in schoolwork, for example in Computing lessons or art homework about AI-generated images. All AI-generated content must be properly attributed
- The Department 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. We understand that technology, and risks and harms

related to it, evolve, and change rapidly and we will carry out regular reviews of our approach to online safety to consider and reflect the risks to our pupils.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the Trust's policies. Policies can be located on the Trust website and individual schools, on their own respective websites. Hard copies of all policies can be made available upon request.

5. Staff (including those involved in governance, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The Trust's IT provider (School Care) manage access to the Trust's ICT facilities and materials for staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the Trust's IT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should seek permission from the file owner in the first instance. If they are not sure who the owner is, a ticket must be logged with IT.

The Trust provides the necessary computer equipment to help staff perform their role. If staff require additional IT equipment, staff should raise this with their line manager. IT equipment that has not been purchased by the Trust will not be connected to the Trust network. **All IT hardware** (Computers, tablets, mobile phones and other devices)must be procured via the Director of Finance in conjunction with the IT provider (School Care).

The disposal of ICT equipment will be arranged by the IT department in conjunction with the Director of Finance in line with the Trust financial procedures manual and with due regard to legal (software compliance, data protection) and environmental issues, ensuring that the appropriate hardware and software registers are updated.

The IT provider is responsible for moving any ICT equipment, whether within an office or to another ILP school. This is to ensure that the Trust's asset register is maintained correctly, equipment is moved safely, and any unwanted stock is disposed of following Waste Electrical and Electronic Equipment (WEEE) directives.

All hardware upgrades to Trust equipment should be performed by the IT Department to ensure warranties remain valid and parts are not ordered when they are already in stock.

Upon leaving the Trust staff are required to return all Trust equipment and accessories that have been provided to them to the IT department. Any personal equipment that has been authorised for Trust use (i.e. configuration of a personal mobile for Trust email) must also be taken to IT for the removal of Trust data.

5.1.1 Use of phones and email

The Trust provides each member of staff with an email address.

This email account should be used for work purposes only. Multi-factor authentication is required on Trust devices.

All work-related business should be conducted using the email address the Trust has provided.

Staff must not share their personal email addresses with parents/carers and pupils and must not send any work-related materials using their personal email account.

All staff with IT access must complete cyber security training on induction and annually as provided by the Trust.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be marked as such or encrypted, so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Data Protection Officer (DPO) immediately and follow the Trust data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the Trust to conduct all work-related business.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

Trust phones should not be used for personal matters, except in emergency circumstances.

Staff who are provided with a Trust mobile phone as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4 and as below:

- Devices must be configured with a keypad password to protect the phone contents and prevent tampering by unauthorised sources.

- Using mobile devices abroad is expensive so please consider using other forms of communication i.e. texts or instant messages. Trust devices should not be used abroad without advance permission from the Director of Finance or CEO.
- To reduce overseas (AKA roaming) charges a specialist bundle can be added to handsets. If staff frequently travel abroad for their role, then please contact Finance.
- Staff should avoid phone or text premium lines (those that start with 0906 etc.) which incur high call charges.
- Where excessive use occurs, staff may be required to reimburse the Trust if usage is not Trust related.
- Staff are advised to back up the contents of their mobile devices periodically using the appropriate mobile phone software.
- If a device is lost or stolen, staff must report this to the IT Helpdesk as soon as this is known. If the item is stolen, staff should report it to the local police authority, obtain a crime report number and submit it to ICT.
- Trust handsets have management applications/settings so the device can be remotely wiped should the device be lost.
- For safeguarding reasons calls for work purposes should not be made on personal devices unless they contain a Trust SIM card.

5.2 Personal use

Staff are permitted to occasionally use Trust ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The CEO/Headteacher may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during pupil contact time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the Trust's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the Trust's ICT facilities for personal use may put personal communications within the scope of the Trust's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff should not use their personal devices to store information about pupils e.g. photos, parent contact numbers.

Staff should be aware that personal use of ICT (even when not using Trust ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the Trust's guidelines on use of social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal Devices

The following section relates to the use of:

a) Trust SIMs in handsets owned by staff or
b) downloading data to personally owned devices.

Staff will be permitted to use their own personal device under the conditions below:

- When using any personal device for any Trust-related work, the device must be protected by a password or passcode.
- When connecting a personal device to the Trust email system, staff consent to policies being automatically pushed to their handset to help protect Trust data.
- Policies include, but are not limited to, the following:
  - the device is always protected by multi-factor authentication
  - Trust data is encrypted
  - Devices are kept up to date on the latest operating system
- Staff agree to always protect their handset with multi-factor authentication
- Staff will take personal responsibility for resetting passwords on their device. The Trust has no control over resetting passwords on personal devices. If a password is forgotten, staff will need to resolve the issue themselves. We advise staff to familiarise themselves with their device password recovery process prior to device configuration.
- Staff will notify the IT Support and the Finance Department immediately if a device is compromised i.e. lost, stolen etc.
- To protect Trust data, all contents of a handset may be remotely wiped should the security of Trust data be compromised i.e. a device is lost or stolen.
- Upon leaving the Trust's employment staff agree to bring any personal device(s) configured for Trust email to the IT Support where they will remove the account configuration and any Trust email from the device(s).
- Staff are responsible for maintaining their own device and the Trust will not reimburse staff for a replacement (should the personal device be lost, damaged etc.) or be liable for additional equipment/extras i.e. chargers.
- Staff are responsible for using their own handset although IT Support will gladly assist providing doing so does not interfere with or prevent us supporting the Trust. We strongly advise that staff regularly backup their device through built in phone functionality and enable any "Find My Phone" feature to assist should the device be lost.
- Staff understand that downloading of Trust data will cause an increase to phone data usage and it is their responsibility to arrange a suitable data tariff to accommodate this usage increase. We recommend a data tariff of 1 GB per month will be needed just for Trust email, but heavy email users may require, a larger data tariff.

- Staff are aware that downloading Trust email when abroad will be significantly more expensive than when in the UK. We advise staff do not download Trust email when abroad, turning off the service before departure unless staff have configured a suitable data tariff to accommodate the increased costs or use wireless networks.
- That staff agree to pay for data tariffs required to accommodate downloading of email and that data cost will not be reimbursed by the Trust. If staff, make regular Trust calls then a Trust handset or Sim card should be requested initially via their Line Manager who will pass the request to central finance.
- This service may be removed at any time if the Trust deems it appropriate i.e. changes in the technology break data protection regulations.

5.2.2 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see Appendix 1).

5.3 Remote access

We allow staff to access the Trust's ICT facilities and materials remotely via SharePoint. This is managed by School Care. Staff will need to login user their Trust email and password.

Staff accessing the Trust's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the Trust's ICT facilities outside the organisation and must take such precautions as School Care, the CEO/Headteacher may require against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

5.4 School social media accounts

The Trust and schools have designated social media accounts. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The Trust has guidelines for what may and must not be posted on its social media accounts, including in relation to images of pupils. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

5.5 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the Trust reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited

- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

In our Trust, we use Netsweeper (which powers Broadband4) for filtering and reporting. This fully complies with all requirements in relation to:

- being a member of Internet Watch Foundation (IWF)
- Being signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

The institution reserves the right to perform inline Secure Sockets Layer (SSL) inspection as part of the provision of internet access within the organisation. SSL inspection requires the deployment of an SSL certificate and as such without the certificate access to SSL encrypted sites will be blocked. It should be assumed that credentials and potentially sensitive information transmitted over the institution's internet connection could be readable to institution staff.

We recognize the importance of clear roles and responsibilities in managing filtering and monitoring systems through:

Regular Review of Provision:

To maintain the effectiveness of our filtering and monitoring systems, we are committed to conducting at least annual reviews that are documented. These reviews allow us to assess the performance and suitability of our current provision and make necessary adjustments to ensure the continued protection of our pupils. The template for these reviews can be found in the local governance and ILP Safeguarding Resources folders.

Blocking of Harmful and Inappropriate Content:

We prioritise the safety of our students by implementing measures to effectively block access to harmful and inappropriate content. It is our goal to strike a balance between maintaining a secure online environment and minimizing any disruptions to teaching and learning activities.

Effective Monitoring Strategies:

To proactively address potential risks and threats, we establish monitoring strategies that align with our safeguarding needs. These strategies will enable us to promptly identify and respond to any concerning online activities or content.

Further information is provided below:

Filtering and monitoring system:	How this meets the monitoring standards:
Our named person for the responsibility in managing our filtering and monitoring systems.	Name of DSL: Rebecca Fisher Oversees: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems
Our filtering system blocks harmful and inappropriate content, without unreasonably impacting teaching and learning.	We do this by: • our filtering system is a member of Internet Watch Foundation (IWF) • they are signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) • they block access to illegal content including child sexual abuse material (CSAM) All Staff will report if: • they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material
Our school's monitoring strategies meet our safeguarding needs.	We do this by: • the monitoring system reviews user activity on school devices effectively. • This allows us to take action; and the response recorded on CPOMs.

The Trust monitors ICT use in order to:

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

Those involved in governance are responsible for making sure that:

- The Trust meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The Trust Board will appoint a named senior leader with responsibility for filtering and monitoring in each setting (the DSL).

This individual will:

- oversee annual reviews of filtering and monitoring effectiveness;
- receive reports on monitoring concerns;
- ensure staff receive relevant training;
- work alongside the Headteacher and IT provider;
- ensure systems remain compliant with DfE Filtering and Monitoring Standards.

Records of annual reviews and testing will be retained

All staff must receive safeguarding and child protection training, including online safety, filtering and monitoring responsibilities, at induction and at least annually thereafter

Where appropriate, staff may raise concerns about monitored activity with an individual school's DSL and the Trust IT provider as appropriate.

6. Pupils

6.1 Access to ICT facilities

The Trust will provide pupils with an account to be able to access appropriate learning, apps, files and folders in school, on any Trust device. Note – From September 2026, it is a DfE expectation that all schools should be mobile phone-free environments by default; anything other than this should be by exception only.

6.2 Search and deletion

Under the Education Act 2011, the Headteacher, and any member of staff authorised to do so by the Headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out (see school behaviour policy) **and/or**

- Is evidence in relation to an offence
- This includes, but is not limited to:
- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from Headteacher or a designated safeguarding lead
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Where appropriate, seek the pupils' consent
- The authorised staff member should:
- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available in the school behaviour policy
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

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

If inappropriate material is found on the device, it is up to the DSL in discussion with the Headteacher, to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

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

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

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school behaviour policy

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the Trust complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy if a pupil engages in any of the following **at any time** (even if they are not on Trust premises):

- Using AI wearables or a mobile phone during the school day including during lessons, the time between lessons, breaktimes and lunchtime, unless by an agreed exception e.g. medical useage
- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust or school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate. Consensual and non-consensual creation, possession, sharing or distribution of nude or semi-nude images, including images generated, altered or manipulated using artificial intelligence technologies.
- Activity which defames or disparages the Trust, school, or risks bringing either into disrepute
- Sharing confidential information about the Trust, school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the Trust's ICT facilities
- Causing intentional damage to the Trust's ICT facilities or materials

- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Sanctions are detailed in the school behaviour policy.

7. Parents/carers

7.1 Access to ICT facilities and materials

Parents/carers do not have access to the Trust's ICT facilities as a matter of course.

However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the Trust's facilities at the Headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

Parents/carers are strictly prohibited from wearing operational AI recording devices when inside the school gates, attending school assemblies, visiting classrooms, or watching school events.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents/carers to sign the agreement in Appendix 2.

7.3 Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in an appropriate manner.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

8. Data security, including energy consumption

The Trust is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its

computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber threats and attack methods

Staff, pupils, parents/carers and others who use the Trust's ICT facilities, should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the Trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Staff passwords must adhere to the following policy:

i. contain a minimum of 7 characters, ideally 12 where technically possible
ii. be unique to each service;
iii. not be shared;
iv. be stored securely using an approved password manager;
v. be protected through multi-factor authentication where available
vi. avoid dictionary words or words that could be associated to the individual (i.e. pet name, date of birth, child names etc.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

All staff will use the password manager to help them store their passwords securely. Teachers will keep pupils' passwords in a secure location in case pupils lose or forget their passwords.

8.2 Software updates, firewalls and anti-virus software

All of the Trust's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the Trust's ICT facilities.

Any personal devices using the Trust's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the Trust's data protection policy. Staff should understand that data protection legislation does not prevent information sharing where there is a safeguarding concern. Concerns about sharing information must never prevent action being taken to safeguard a child. Information should be shared proportionately, lawfully and in the child's best interests.

8.4 Access to facilities and materials

All users of the Trust's ICT facilities will have clearly defined access rights to Trust systems, files and devices.

These access rights are managed by the Trust IT provider.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the person who gave them access and raise a ticket with IT immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

8.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headteacher or CEO.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by our IT provider.

8.6 Energy Consumption

The Trust is committed to minimising energy consumption and to help reduce energy waste, please adhere to the following where practical:

- Turn off IT equipment at the end of each day that is not being actively used, including PCs, projectors, screens, whiteboards, printers, photocopiers, and ancillary equipment.
- Configure PC power options in control panel to improve energy efficiency.
- Reduce the brightness on the PC screen - monitors running on half brightness consume only three quarters of the power.
- When staff leave a room at the end of the day, ensure the ICT equipment is turned off but left connected for the next person.
- Consider whether printing/photocopying a document is necessary.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The Trust will:

- Work with those involved in governance and IT Support to make sure cyber security is given the time and resources it needs to make the Trust secure
- Provide mandatory training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **Proportionate:** the Trust will verify this using a third-party audit (such as 360 degree safe) to objectively test that what it has in place is effective
    - **Multi-layered:** everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when the Trust needs to update its software
    - **Regularly reviewed and tested:** to make sure the systems are as effective and secure as they can be
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT provider.
- Make sure staff:
    - Login to our network and SharePoint working from home
    - Enable multi-factor authentication where they can, on things like Trust email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the Trust has the right level of permissions and admin rights
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the Trust will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

10. Internet access

The Trust's wireless internet connection is secure.

Filtering is in place. If the filtering hasn't identified a site of concern (or appropriate sites have been filtered in error), a ticket should be raised with the IT provider.

Separate connections are in place for parents/carers/the public – following authorisation by the Headteacher, guest access is created by the school administrator for a limited period.

10.1 Pupils

Pupils will access the Trust Wi-Fi using their Trust provided login, on a Trust device.

10.2 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the Headteacher.

The Headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's WiFi in order to fulfil the purpose of their visit (for instance, an Ofsted inspection or to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The CEO and IT provider monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Trust.

This policy will be reviewed annually by the Trust Board.

12. Related policies

This policy should be read alongside the following policies:

- Child Protection & Safeguarding Policy
- Behaviour Policy
- Disciplinary Policy
- Staff Code of Conduct Policy
- Data protection Policy

Changes History Table

Version	Date	Amended by	Approved By	Summary of Changes
4	September 2026	Director of Safeguarding and School Operations (Trust DSL) and reviewed by Executive Team	Trustees	• Alignment with KCSIE 2026 and latest DfE guidance. • Comprehensive AI and generative AI safeguards added. • Restrictions on AI wearables, smart glasses and recording devices. • Mobile phone-free school expectation introduced in line with DfE requirement. • Enhanced filtering and monitoring governance arrangements. • Updated cyber security and password requirements. • Headteacher terminology replacing Principal. • New safeguarding wording on information sharing and AI-generated imagery.

13. Appendix 1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

10 guidelines for Trust staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image remains professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be happy for pupils or parents to see
6. Don't use social media sites during work hours, except for work business
7. Don't make comments about your job, your colleagues, our Trust or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the Trust on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify the Headteacher and their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the Headteacher and DSL about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, the Headteacher should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

14. Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers

Name of parent/carer:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our Official Facebook Page

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp). The school does not sanction any unofficial groups and will not mediate any issues that arise in such groups.

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers

I acknowledge that:

- Smart eyewear, AI-enabled wearables, body-worn recording devices or other technologies capable of recording audio, video, images or biometric data must not be used on Trust premises without explicit authorisation.

Signed:	Date:

15. Appendix 3: Acceptable use agreement for older pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers
Name of pupil:

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a staff member being present, or without a staff member's permission
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video
- Share my password with others or log in to the school's network using someone else's details
- Bully other people
- Use AI tools and generative chatbots (such as ChatGPT or Google Gemini):
    - During assessments, including internal and external assessments, and coursework
    - To present AI-generated text or imagery as my own work

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

I will not use my mobile phone anywhere on the school site, including during lessons, the time between lessons, breaktimes, lunchtimes and on the playground, field etc. at the beginning and end of the school day. I will not wear AI glasses, smart watches anywhere on school grounds, during the school day, or during school sanctioned transport.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

16. Appendix 4: Acceptable use agreement for younger pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not:

- Use them without asking a staff member first, or without a staff member in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes
- Share my password with others or log in using someone else's name or password
- Bully other people
- Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Gemini, to create images or write for me, and then submit it as my own work

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I will keep my mobile phone switched off and out of sight at all times when I am at school.

I will not wear or use AI glasses or smart watches while I am at school or on school transport.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

17. Appendix 5: Acceptable use agreement for staff, those involved in governance, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet:
agreement for staff, those involved in governance, volunteers and visitors

Name of staff member/person involved in governance/volunteer/visitor:

When using the Trust's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the Trust's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the Trust's network
- Share my password with others or log in to the Trust's network using someone else's details
- Share confidential information about the Trust, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote any private business, unless that business is directly related to the Trust

I understand that the Trust will monitor the websites I visit and my use of the Trust's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT provider know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the Trust's ICT systems and internet responsibly and ensure that pupils in my care do so too.

I will not wear personal smart eyewear or AI recording devices during teaching hours, duty periods, or when supervising pupils unless they are being used as part of a lesson.

Signed (staff member/person involved in governance/volunteer/visitor)	**Date:**

Appendix 6: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.

TERM	DEFINITION
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.

TERM	DEFINITION
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

18. Appendix 7 Data Protection Impact Assessment (DPIA) enquiry form

Data Protection Impact Assessment (DPIA) enquiry form

Please use this form to notify the data protection officer (DPO) that you are considering entering into a purchase or contract with a third party that would involve sharing or processing personal data. Please send to DPO@ILPartnership.org and include the IT department if you wish.

Your name _____

Date form completed _____

Date form sent to data protection officer (DPO) _____

	DPOs: make any comments here
Please give a brief description of the project you are considering *(For example, purchase of online apps, or provision of IT services from an external provider)*	
Will this project involve the processing or sharing of personal data? YES / NO *(Personal data is defined as any information that could identify individuals, such as names, contact details, user names or ID numbers)*	
If 'YES', please give a description of what personal data you will be processing or sharing, and the scale of this processing	

Inspire Learning Partnership is a charitable company limited by guarantee registered in England and Wales with company number 9202445

Will this project involve the processing or sharing of sensitive personal data? YES / NO *(Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometrics, physical or mental health, sexual orientation, or photographs)*	
If 'YES', please give a description of what sensitive data you will be processing or sharing, and the scale of this processing	

Please return this form to your DPO.

19. Appendix 8: Subscriptions, Contract, SLA enquiry form

Subscriptions, Contract, SLA enquiry form

Please use this form to notify the Trust Operations Officer (TOO) that you are considering entering into a purchase or contract with a third party, subscription, software purchase or SLA.

Please send to DPO@ILPartnership.org and include the IT department if you wish.

Your name _____

Date form completed _____

Date form sent to data protection officer (DPO) _____

	TOOs: make any comments here
What is the product called?	
What is the name of the supplier who will be providing the agreement/product?	

Inspire Learning Partnership is a charitable company limited by guarantee registered in England and Wales with company number 9202445

What is the purpose of this agreement/product for the School/Trust?	
What Key Stage is the agreement/product for? Whole/Partial?	
What is the cost of the agreement/product?	
Are you aware of other Schools within the Trust using this agreement/product?	
Who is the Lead Contact?	
Has the Headteacher agreed in Headteacher to the use of this agreement/product?	

Please return this form to your DPO.