**DATA Sharing Agreement**

Data sharing agreement between the Metropolitan Police Service and education establishments in a Safer School Partnership.

**[Insert school name]**



**DSA Ref:** General Registry File Ref Number – [Insert Number - obtained from Records Management via form 911.]

|  |  |
| --- | --- |
| Protective Marking | Official |
| Title and Version | Data sharing agreement between the Metropolitan Police Service and education establishments in a Safer School Partnership. |
| Version | 1.3 |
| Purpose | Guidance and agreement document |
| Relevant to | Safer Schools Officers, Safer Schools supervisors, Youth Offending Teams, education establishments |
| Summary | A data sharing agreement between the Metropolitan Police Service and education establishments in a Safer School Partnership.  See the SSP protocol for partnership working practices. |
| Author | [Insert Author] |
| Borough/BCU | [Insert borough/BCU] |
| Organisation | Metropolitan Police Service |

Table of Contents

[1 Purpose of the Data Sharing Agreement 4](#_Toc29826075)

[2 Definitions 5](#_Toc29826076)

[2.1 Safer School Partnership (SSP) 5](#_Toc29826077)

[2.2 Partner / Parties 5](#_Toc29826078)

[2.3 Personal data 5](#_Toc29826079)

[2.4 Special category data 5](#_Toc29826080)

[3 Background 6](#_Toc29826081)

[4 Sharing Data 7](#_Toc29826082)

[4.1 The police 7](#_Toc29826083)

[4.2 The educational establishment 8](#_Toc29826084)

[4.3 Data to be shared 8](#_Toc29826085)

[4.4 Benefits 9](#_Toc29826086)

[4.4.1 Benefits to the police 9](#_Toc29826087)

[4.4.2 Benefits to the educational establishment 9](#_Toc29826088)

[4.4.3 Benefits to the school community 10](#_Toc29826089)

[5 MPS Privacy Management and Security Framework 11](#_Toc29826090)

[5.1 Request for data within SSPs 11](#_Toc29826091)

[5.2 How the police handle a request for data 11](#_Toc29826092)

[5.3 Personal data security classification 11](#_Toc29826093)

[5.4 Confidentiality and Vetting 11](#_Toc29826094)

[5.5 Methods of Data Transfer 12](#_Toc29826095)

[5.5.1 Physically held by MPS 12](#_Toc29826096)

[5.5.2 Electronically held by MPS 12](#_Toc29826097)

[5.6 MPS Data Storage 13](#_Toc29826098)

[5.6.1 Educational establishments Building and Perimeter Security 13](#_Toc29826099)

[5.6.2 Hard Copy 13](#_Toc29826100)

[5.6.3 Storage of Electronic Data on educational establishments System 13](#_Toc29826101)

[5.7 Business Continuity 13](#_Toc29826102)

[5.7.1 Electronically 14](#_Toc29826103)

[5.7.2 Hard Copy 14](#_Toc29826104)

[5.8 MPS Data destruction / disposal 14](#_Toc29826105)

[5.8.1 Electronic Data 14](#_Toc29826106)

[5.8.2 Hard Copy 14](#_Toc29826107)

[5.9 Reporting Security Incidents and Breaches of the Agreement 14](#_Toc29826108)

[5.9.1 MPS 14](#_Toc29826109)

[5.9.2 Educational establishment reporting 14](#_Toc29826110)

[5.10 Compliance 15](#_Toc29826111)

[5.11 Review 15](#_Toc29826112)

[6 Legal basis for sharing data 16](#_Toc29826113)

[6.1 Data protection Act 2018 18](#_Toc29826114)

[6.2 First Principle – Data Protection 18](#_Toc29826115)

[6.2.1 Children Act 2004 18](#_Toc29826116)

[6.2.2 Education Act 2002 19](#_Toc29826117)

[6.2.3 Common Law 19](#_Toc29826118)

[6.2.4 Duty of Confidence 20](#_Toc29826119)

[6.2.5 Fair Processing 20](#_Toc29826120)

[6.2.6 Legitimate Expectation 21](#_Toc29826121)

[6.2.7 Human Rights - Article 8: The right to respect for private and family life, home And correspondence 21](#_Toc29826122)

[6.2.8 Schedule 8, Part 3 Data Protection Act 2018 22](#_Toc29826123)

[6.3 Second Principle – Data protection 23](#_Toc29826124)

[6.3.1 How the agreement complies with the second data principle 23](#_Toc29826125)

[6.4 Third Principle – Data Protection 23](#_Toc29826126)

[6.4.1 How the agreement complies with the third data principle 24](#_Toc29826127)

[6.5 Fourth Principle – Data protection 24](#_Toc29826128)

[6.5.1 How the agreement complies with the fourth data principle 24](#_Toc29826129)

[6.6 Fifth Principle – Data Protection 24](#_Toc29826130)

[6.6.1 How the agreement complies with the fifth data principle 24](#_Toc29826131)

[6.7 Sixth Principle – Data protection 25](#_Toc29826132)

[6.7.1 How the agreement complies with the sixth data principle 25](#_Toc29826133)

[6.8 Freedom of Information Act and Right of Access Requests 25](#_Toc29826134)

[7 Agreement to abide by this arrangement 26](#_Toc29826135)

[MPS 26](#_Toc29826136)

[Educational Establishment 26](#_Toc29826137)

[Appendices 27](#_Toc29826138)

[Appendix A: Data Sharing Request Form 27](#_Toc29826139)

# 1 Purpose of the Data Sharing Agreement

This agreement was developed to facilitate the Safer School Partnership (SSP) by:

* Defining the specific purposes for which the signatory parties have agreed to share data.
* Describing the roles and structures that will support the exchange of data between parties.
* Setting out the legal gateway through which the data is shared, including reference to the Human Rights Act 1998 and the common law duty of confidentiality, section of the Children Act 2004, Crime and Disorder Act 1998 and statutory guidance.
* Describing the security procedures necessary to ensure that compliance with responsibilities under the Data Protection Act and party specific security requirements.
* Outlining the personal and/or special category information to be shared.
* Describing how the rights of the data subject(s) will be protected as stipulated under the Data Protection laws (General Data Protection Regulations (GDPR), Law Enforcement Directive and the Data Protection Act).
* Describing how this arrangement will be monitored and reviewed.

In addition, completion of this document will ensure that the Metropolitan Police Service can meet the data sharing requirements of the Guidance on the Management of Police Information (MoPI).

**The signatories to this agreement represent the following parties:**

Metropolitan Police Service - [Name of borough]

[Name of education establishment]

|  |
| --- |
| **RELEVANT LEGISLATION**  Working together to safeguard children (*Statutory guidance on inter-agency working to safeguard and promote the welfare of children*): <https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>  Section 17 Children Act 1989 (*Provision of services for children in need, their families and others*): <http://www.legislation.gov.uk/ukpga/1989/41/section/17>  Section 47 Children Act 1989 (*Local authority’s duty to investigate*): <http://www.legislation.gov.uk/ukpga/1989/41/section/47>  Section 9A Children Act 2004 (*Targets for safeguarding and promoting the welfare of children*): <http://www.legislation.gov.uk/ukpga/2004/31/section/9A>  Section 10 Children Act 2004 (*Co-operation to improve well-being*): <http://www.legislation.gov.uk/ukpga/2004/31/section/10>  Section 11 Children Act 2004 (*Arrangements to safeguard and promote welfare*): <http://www.legislation.gov.uk/ukpga/2004/31/section/11>  Section 115 Crime and Disorder Act 1998 (*Disclosure of data*): [http://www.legislation.gov.uk/ukpga/2018/37/section/115](http://www.legislation.gov.uk/ukpga/1998/37/section/115)  Data sharing (*Advice for practitioners providing safeguarding services to children, young people, parents and carers*): [https://www.gov.uk/government/publications/safeguarding-practitioners-data-sharing-advice](https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice)  Human Rights Act 1998 (*contents*): [http://www.legislation.gov.uk/ukpga/2018/42/contents](http://www.legislation.gov.uk/ukpga/1998/42/contents)  Data Protection Act 2018 (*contents*): <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>    College of Policing (2014) Management of Police Information: [https://www.app.college.police.uk/app-content/data-management/management-of-police-data/](https://www.app.college.police.uk/app-content/information-management/management-of-police-information/) |

# 2 Definitions

## 2.1 Safer School Partnership (SSP)

An SSP is a formal agreement between a school and the police to work together in order to keep young people safe, reduce crime and the fear of crime and improve behaviour in schools and their communities. The underlying assumption is that by reducing bullying, truancy and exclusions from school, SSPs will affect indirectly on offending and antisocial behaviour.

An SSP is a positive way for the police and all schools to demonstrate their commitment to promoting a safe environment to learn and prevent crime. This will involve a police Safer Schools Officer regularly working at a school or across a number of schools on a full time or part time basis.

The head teacher and their staff retain responsibility for school discipline and most behaviour, with the police providing advice and support as well as a physical presence.

See the SSP protocol for further information.

## 2.2 Partner / Parties

For simplicity, **the educational partner will be referred to as ‘education establishment’ or ‘school’ in this agreement.**

**‘Parties’** is used to refer to both the MPS and the educational establishment.

## 2.3 Personal data

Information relating to a living identified or identifiable individual, including name, address, dob, id number, location data, online identifier or one or more factors specific to someone’s physical, physiological, genetic, economic, cultural or social identity.

## 2.4 Special category data

Data relating to racial, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics, health, sex life / orientation, criminal convictions and offences, related security measures or appropriate safeguards.

# 3 Background

Safeguarding and promoting the welfare of children is defined in statutory guidance as:

* protecting children from maltreatment;
* preventing impairment of children's health or development;
* ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and
* taking action to enable all children to have the best outcomes.

This means that the organisations involved with providing services to children and young people, including all types of Schools, Colleges, Pupil Referral Units (PRU) and the police, need to share data and work together to protect children and young people from harm and help them achieve successful outcomes.

Through this Data Sharing Agreement (DSA), police and education establishments will work to keep pupils/students and staff safe, reduce the risk of young people getting drawn into crime or anti-social behaviour, improve the safety of the site and surrounding area, build positive relationships between pupils/students and police, promote shared values and improve community relations generally within the education establishment and the wider community.

|  |
| --- |
| **RELEVANT LEGISLATION**  Working together to safeguard children (*Statutory guidance on inter-agency working to safeguard and promote the welfare of children*): <https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>  Data sharing (*Advice for practitioners providing safeguarding services to children, young people, parents and carers*): [https://www.gov.uk/government/publications/safeguarding-practitioners-data-sharing-advice](https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice) |

# 4 Sharing Data

**See section 4 for the legal basis for sharing data.**

The purpose of a data sharing arrangement is to enable parties to exchange and share data with each other. A Protocol or Agreement provides a secure framework within which the parties can operate and exchange data rather than having in place an ad hoc system with no obvious guidelines and boundaries. This Agreement provides protection for persons who will be sharing data.

## 4.1 The police

The police will share information with the educational establishment:

* To ensure that the education establishment is aware, where relevant, of pupils/students who have been arrested for offences in order that any risk may be effectively managed.
* To ensure that the education establishment is updated, where relevant, with the investigation stage of an allegation against a student in order that support mechanisms / procedures may be implemented.
* To ensure that Police inform the education establishment of any known anticipated violence within or surrounding their premises, or involving their student/s in order that preventive measures may be implemented.

Safer Schools Officers will check daily police briefings for any data that may be needed for school safety. Police briefing pages **MUST NOT** be forwarded to schools or printed off. The local police intelligence Unit supervisor must be consulted where an officer considers it necessary to exchange police briefing material, such as intelligence of pre disorder and gang fights at a particular school.

The officer for each school will conduct daily and weekly checks to identify young people who have been arrested and attend the school. The officer will inform the school of the circumstances. This is of particular importance where the victim and suspect of an offence attend the same school so that school staff can manage any risks. The officer will assist in this process.

It may be necessary to inform the educational establishment immediately that someone has come to police notice for committing a criminal offence and/or act of disorder to prevent it from happening again.

Data concerning students, who have been arrested for, or suspected of, an offence relating to the carriage of weapons, violence or drugs, may be shared with the school so they may make informed decisions about excluding them or putting control measures in place to manage any risk. Examples of situations where, if deemed appropriate, data may be shared on a case-by-case basis are where an individual was;

* Involved or alleged to be involved in an incident in the locality of the school or travelling to/from the school.
* Involved or alleged to be involved in a violent confrontation, between school students or other parties, at any time where reprisals are feared.
* Arrested in the locality of the school or travelling to/from the school, and cautioned, reprimanded, warned, given a Penalty Notice for Disorder (PND) or charged and attending court.
* Arrested and been given bail conditions that subject would be in breach of if they attended the school.

Other relevant police data about an individual may be shared if deemed necessary. This data may include data from police crime and intelligence systems (i.e. name, address, DOB, bail conditions, court dates) and their history (previous related offences, pre-existing relevant intelligence). For each item of data, clearly list all the data that’s likely to be shared, including personal and special category data types and why the data is essential and what the impact would be if it were not shared.

**All data shared will be recorded on CRIMINT.**

Data will not be shared where the officer cannot justify the sharing of it. Personal details of anyone involved in criminal investigations or any other matter will not be shared unless it is necessary and can be justified.

## 4.2 The educational establishment

The educational establishment will share information with the police:

* To ensure that the police are aware of any anticipated violence in order that preventive measures are implemented.
* To assist police in the identification of pupils/students who are suspected of criminal offence(s) in order for prompt effective outcomes.
* To ensure that the objectives of the Children Act 2004 in securing the welfare of all children is achieved.

In the absence of a Court Order, or enabled by Section 47 of the Children Act 1989, the specifics of the information requested will be assessed in line with the Data Protection Act 2018 and the data Controller will keep a record of

* the request made, and
* the information or personal data disclosed in line with legislation.

This can be done by completing a form.

## 4.3 Data to be shared

Both parties will be sharing both personal data and special category data as defined in the Data Protection Act 2018.

In pursuance of the objectives of the Children Act 2004, the data that may be disclosed in relation to the student(s), to assist with matching persons and incidents and ensuring they are the correct individual could include:

**Personal Identifiers**

1. Name /alias
2. Date of birth
3. Address
4. Gender
5. Ethnicity
6. Physical description
7. Images / video footage

Data relating to criminal offences, anti-social behaviour or other factors that could prevent the child from obtaining the statutory 5 outcomes of the Children Act 2004 which may be shared include:

* Nature of offence
* Nature of data, for example behaviour
* Any known risk

The Police systems that may be interrogated for data are:

* Met Briefing and Tasking System (MetBaTS)
* The Police National Computer (PNC)
* The Criminal Intelligence System (CRIMINT)
* Crime Reporting Information System (CRIS)
* Computer Aided Despatch (CAD) - data relating to incidents reported to police concerning crime and events within the MPS
* Merlin (system the MPS uses to record when children come to police attention)
* Custody Records (NSPIS)
* Custody imaging system
* Youth Offending Team records

## 4.4 Benefits

Sharing data between both parties is essential in achieving the SSP objectives and objectives of the Children Act 2004. Without clear channels of communication, and an agreed Data Sharing Agreement, neither party will be able to manage incidents as effectively.

This agreement will allow for more targeted intervention by both parties. The need for police involvement in education and engagement with young people will be clearly identified.

### 4.4.1 Benefits to the police

By sharing data, Police are better placed to investigate allegations of crime, provide a better service to the victims of crime and reduce the risk of criminal activity escalating.

Support can be provided for young people to deal with situations that may put them at risk of becoming victims of crime, bullying or intimidation.

More positive relationships can be built between young people and the police.

The agreement will also benefit Police in reducing incidents of youth violence.

* Assisting in the identification of suspected offenders will have a positive outcome on reducing youth violence and will assist in preventing repeat offending by implementing both enforcement and supportive measures.
* An increase in engagement and the flow of data and intelligence between education establishments and police, in relation to preventing and reducing crime.
* To ensure the effective joint management of young offenders, or those likely to become offenders without intervention.
* Early identification and support for pupils/students at risk of offending.
* Contributing to wider crime prevention objectives and police supporting education establishments as part of overall neighbourhood policing work.

### 4.4.2 Benefits to the educational establishment

By sharing data, the education establishment will be better placed to effectively deal with and help pupils/students who have been arrested or who are in the Criminal Justice System.

Education establishments will benefit by having up to date data on pupils/students within the criminal justice system. This will enable them to manage any risk posed to that student or any others who may be affected. It will allow appropriate support to be given where required. By effectively managing incidents of anticipated violence, this will increase the safety of both pupils/students and staff.

The sharing of data between parties will enable the education establishments to be better able to discharge their responsibilities in loco parentis, with improved standards of pupil behaviour and attendance.

### 4.4.3 Benefits to the school community

By the effective sharing of data, the benefits to the citizen are very clear. Preventing an anticipated fight between young people will greatly reduce the risk of injury, serious harm or even fatalities. If parties to this agreement work together to prevent such anticipated incidents then the safety of the citizen will increase. By dealing efficiently with allegations of a criminal nature, especially those involving weapons and violence, then the risk of the incident escalating is again reduced, and the safety of the citizen increased.

This agreement will assist in preventing young people from entering the Criminal Justice System through early intervention and engagement with police.

The agreement will support appropriate data sharing between the MPS, educational establishment, parents and carers.

# 5 MPS Privacy Management and Security Framework

## 5.1 Request for data within SSPs

A request for data will be made in writing by completing a data sharing request form (*see Appendix A*). This can be securely emailed, or given to the Safer Schools Officer (PC) or the MPS youth Sergeant in physical form.

The police within the SSP may be required to complete a data request form as per educational establishment policy.

Depending on the request, several police systems may be interrogated by the officer receiving the request – CRIS, CRIMINT, Merlin or PNC.

Should there be a requirement for the school to show other parties the data shared (other than the signatories to this agreement), the school will seek permission from the MPS in writing.

## 5.2 How the police handle a request for data

The data gathered will be provided to the school SPOC and/or Head Teacher. All data shared must be handled according to its security classification.

A record of the personal data disclosed will be created on CRIMINT PLUS by the officer sharing the data at the time the data is supplied (or as soon as possible thereafter). This should include what was shared and the reason for sharing. Any decision not to share data should similarly be recorded along with the reasons for the decision. Where data sharing has been recorded on CRIS, there is no need to then also record on CRIMINT.

There is no requirement for the school to have access to MPS ICT systems.

All data will remain with the European Economic Area (EEA).

## 5.3 Personal data security classification

Personal data to be shared by the Safer Schools Officer will be security marked ‘OFFICIAL SENSITIVE’ in accordance with the Government Security Classification (GSC). In the event that there is a requirement to share material of a different classification, please refer to the Government Security Classification policy. If you have any security questions which can’t be answered by referring to the GSC policy, please contact the [Information Assurance Unit (IAU).](mailto:DOI%20Mailbox%20-%20Security%20Advice)

|  |
| --- |
| **RELEVANT LEGISLATION**  Government Security framework policy: <https://www.gov.uk/government/publications/security-policy-framework> |

## 5.4 Confidentiality and Vetting

The OFFICIAL SENSITIVE data shared through this agreement does not require vetting on the part of school staff, provided it is shared on a ‘need-to-know basis’. All individuals working within an education environment have been subject to Enhanced Disclosure and barring Service (DBS) checks (previously Criminal Records Bureau (CRB) checks).

Where OFFICIAL SENSITIVE data is being shared; vetting is not mandatory but access must always be limited on a strict “need-to-know” basis (unless there are national security implications, in which case a Counter Terrorist Check [CTC] is required). The educational establishment must confirm that employees who will access shared data will have a need-to-know that data, and that they have provisions in place to ensure that unauthorised dissemination or copying by their staff does not occur.

|  |
| --- |
| **RELEVANT LEGISLATION**  DBS checks (previously CRB checks): <https://www.gov.uk/disclosure-barring-service-check/overview> |

## 5.5 Methods of Data Transfer

Data will be requested and shared by the following routes:

* Verbally (providing a record is created). During face to face meetings between the Safer Schools Officer and Specific Points of Contact (SPOC) at the school.
* Secure email (you must clarify which secure email option that you will be using , .pnn, .gsi, .cjsm, Egress and nhs.net are examples of secure email. .gov.uk and nhs.uk are not secure. For further information about secure email, please consult ‘Use of Secure Email Guidance’ on the IAU intranet page).
* If the school does not have secure email then data will be passed by hand.

The expectation is that the sharing of data will be a regular process, often dictated by events and thus there is no specific requirement for a regular timed process.

“Soft” intelligence, e.g. Safer Schools Officer hearing a conversation about possible disruption to a lesson, may be passed verbally to a relevant member of staff.

### 5.5.1 Physically held by MPS

Where OFFICIAL SENSITIVE information is concerned, the information will be kept within a secure location with a managed and auditable access control system that the general public have no access to.

* Data will be moved by a trusted person in a closed container or package. E.g. A closed folder or closed box.
* Data will be moved by post or courier in a sealed package with no protective markings showing (other than PERSONAL or PRIVATE). It will be addressed to a specified individual within the educational establishment by name or appointment (add job title).

### 5.5.2 Electronically held by MPS

* Data with a classification of up to the OFFICIAL SENSITIVE must be transferred using secure email. (Please note that pnn, .gsi, Egress, .cjsm, and nhs.net are examples of secure email, whilst, .gov.uk and nhs.uk are not secure). For further data about secure email, please consult ‘Use of Secure Email Guidance’ on the IAU intranet site. If the data has a higher protective marking, please seek advice from the MPS Information Assurance Unit (IAU).
* If data will be stored on removable media, these will be encrypted to government standards. Only the government encrypted MPS approved Datashur USB may be used. These are available on PSOP. **CDs are no longer acceptable.**
* Via telephone, provided a record is subsequently made. It is prudent to use guarded speech and keep conversations short.
* Avoid the use of fax for transferring protectively marked data as it is not secure.

|  |
| --- |
| **RELEVANT LEGISLATION**  Common Technology Services (CTS) (*Secure email blueprint*): <https://www.gov.uk/guidance/common-technology-services-cts-secure-email-blueprint> |

## 5.6 MPS Data Storage

### 5.6.1 Educational establishments Building and Perimeter Security

Where OFFICIAL SENSITIVE data is concerned; the data will be kept within a secure location with a managed and auditable access control system that the general public have no access to.

### 5.6.2 Hard Copy

OFFICIAL SENSITIVE MPS data will be stored in a locked container within a secure premise with a managed access control. Access to data will be limited to those with a genuine “need-to-know”. When the documents are not being used they will be locked away.

### 5.6.3 Storage of Electronic Data on educational establishments System

Where data is being kept electronically, educational establishment confirm that system access controls are in place (i.e. username & password / keeping permissions to a minimum) to those who have a genuine “need-to-know”. It has been confirmed that access to the data can be audited. When the documents are not being used they will be locked away.

## 5.7 Business Continuity

The Safer Schools Officer will be the MPS single point of contact for each school. Each educational establishment will have a nominated SPOC, which will usually be the head teacher or a member of the Senior Leadership Team.

Deputies will be assigned in the event of the SPOCs being unavailable. If data cannot be transferred by the normal method, then the default mode of delivery will be via hand between the SPOCs.

If the need arises for data shared within this agreement to be backed up either electronically or with the movement of physical files, then the responsible party must ensure that the appropriate storage and protection measures are in place.

### 5.7.1 Electronically

If data is backed up electronically via disc, hard drive, or any mobile device, then the appropriate level of encryption and or password requirements must be in place. This should be followed by the media used being stored in a physical location that has a level of security appropriate to the level that the data held is graded to.

### 5.7.2 Hard Copy

If data shared under this agreement must be moved from its usual secure location, which is in accordance with the level of security required by this agreement, then any move temporary or permanent must provide the same level of security in storage as originally agreed and stated in this document.

Whilst the educational establishment may have their own security standards & protocols, where MPS data is concerned the relevant security standards set out by the GSC for transmitting, storing and disposing data must be adhered to at all times.

## 5.8 MPS Data destruction / disposal

The guidance below relates to the disposal of OFFICIAL SENSITIVE information, including papers and electronic information*.*

### 5.8.1 Electronic Data

Data will be overwritten using an approved software utility or will be disposed of through the physical destruction of the computer media.

### 5.8.2 Hard Copy

Data provided by the educational establishment in hard copy will be destroyed when it is no longer useful or relevant under the agreement by being shredded, or returned to the MPS contact for destruction through the MPS OFFICIAL SENSITIVE waste system.

## 5.9 Reporting Security Incidents and Breaches of the Agreement

### 5.9.1 MPS

Security breaches, including misuse of MPS information must be reported to the MPS Single Point Of Contact (Safer Schools Sergeantt) without undue delay of occurring/or no later than 24 hours after becoming aware of it. This is to allow the MPS to risk assess the security incident or breach of the Agreement.

The nominated MPS individual must immediately inform the MPS Information Assurance Unit (IAU) of any security incident or breach of this agreement, including unauthorised disclosure or loss of data, by emailing ‘IAU Mailbox - Security Incidents’.

### 5.9.2 Educational establishment reporting

Security breaches must be reported without undue delay in accordance with education establishment’s Data Protection Policy and Data Incident Response Policy. The educational establishment Principal and Data Champion are to be informed in the first instance, prior to escalation to the DPO.

Security breaches (including misuse or unauthorised disclosure) are covered by the educational establishment’s internal disciplinary procedures. If misuse is found, there should be a mechanism to facilitate an investigation into initiating criminal proceedings.

## 5.10 Compliance

The educational establishment is responsible for ensuring the security controls are implemented and staff are aware of their responsibilities under the Data Protection Act 2018 and the Children Act 2004.

Both parties agree where necessary to allow peer-to-peer reviews to ensure compliance with the security section of this DSA. Compliance with these security controls will be catered for in the periodic reviews of the DSA.

## 5.11 Review

In accordance with the Guidance on the Management of Police Information (MoPI) this agreement will be reviewed six months after implementation and annually thereafter.

|  |
| --- |
| **RELEVANT LEGISLATION**  College of Policing (2014) Management of Police Information: [https://www.app.college.police.uk/app-content/data-management/management-of-police-data/](https://www.app.college.police.uk/app-content/information-management/management-of-police-information/) |

# 6 Legal basis for sharing data

**The Data Protection Act 2018**

Acts as a framework on how to process and share personal data with trusted partners.

* Schedule 1, Part 2 and Part 3 lists various conditions which, when fulfilled, allow for lawful processing of personal & special category data.
* Schedule 8, Part 3 lists conditions which are applicable when sharing special category data.

In order to process and share personal data, **the following Substantial Public Interest Condition will be satisfied**.

* *Preventing or detecting unlawful acts Section 10(1)(2)(3);*
* *Safeguarding of children and of individuals at risk Section 18(1)(2)(3)(4).*

*Access this link for the relevant sections of the DPA 2018 Act*

<http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

Schedule 1, Part 2, Data Protection Act 2018

In addition to the legal criteria set out above, the data sharing arrangement must satisfy at least one condition in Schedule 2 of the Data Protection Act in relation to personal data.

The sharing of personal data in this agreement satisfies the following conditions of Schedule 2.

* The data subject has consented to the processing [1]

This will be the relevant condition where consent has been sought from a victim or a witness to share data with their school for their benefit.

**or**

* The processing is necessary for the exercise of any function conferred under any enactment [5(b)]

The enactment for this data sharing agreement which makes this condition relevant is Section 11 Children Act 2004 and Section 175 Education Act 2002.

**or**

* The processing is necessary for the legitimate interests of the data controller [6(1)]

This is the condition where a Common Law Policing Purpose has been identified for sharing personal data.

Set out above, the data sharing arrangement must satisfy at least one condition in Schedule 2 of the Data Protection Act in relation to personal data.

The sharing of personal data in this agreement satisfies the following conditions of Schedule 2.

* The data subject has consented to the processing [1]

This will be the relevant condition where consent has been sought from a victim or a witness to share data with their school for their benefit.

**or**

* The processing is necessary for the exercise of any function conferred under any enactment [5(b)]

The enactment for this data sharing agreement which makes this condition relevant is Section 11 Children Act 2004 and Section 175 Education Act 2002.

**or**

* The processing is necessary for the legitimate interests of the data controller [6(1)]

This is the condition where a Common Law Policing Purpose has been identified for sharing personal data.

In order to process and share personal data, **the following additional condition relating to criminal convictions** in Schedule 1, Part 3 are satisfied.

* *Consent Section 29;*
* *Protecting individual’s vital interests Section 30(a)(b);*
* *Extension of conditions in Part 2 of this Schedule referring to substantial public interest Section 36.*

*Access this link for the relevant sections of the DPA 2018 Act*

<https://publications.parliament.uk/pa/bills/cbill/2017-2019/0190/18190.pdf>

Schedule 8, Part 3, Data Protect Act 2018

In order to process and share special category data, **the following special category data** in Schedule 8, Part 3 will be satisfied.

* *Statutory etc. purposes Section 1*(a)(b);
* *Safeguarding of children and of individuals at risk Section 4(1)(2)(3)(4);*
* *Personal data already in the public domain Section 5;*

*Access this link for the relevant sections of the DPA 2018 Act*

<https://publications.parliament.uk/pa/bills/cbill/2017-2019/0190/18190.pdf>

**If Schedule 8, Part 3 is applicable, state which condition(s) is/satisfied and elaborate.**

*If the information intended for sharing is not special category data state –*

“No special category data will be shared for the purpose of this agreement”.

## 6.1 Data protection Act 2018

Sharing of personal data can take place only if the sharing complies with the Six Data Protection Principles.

|  |
| --- |
| **RELEVANT LEGISLATION**  Data Protection Act 2018 (*contents*): <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>  Part 3, Chapter 2, Data Protection Act 2018 (*The principles*): <http://www.legislation.gov.uk/ukpga/2018/12/part/3/chapter/2/enacted> |

## 6.2 First Principle – Data Protection

The first data protection principle states that data must be processed lawfully and fairly.

|  |
| --- |
| **RELEVANT LEGISLATION**  Part 3, Chapter 2, Section 35(1) Data Protection Act 2018 (*The first principle*): <http://www.legislation.gov.uk/ukpga/2018/12/section/35/enacted>  Section 11 Children Act 2004 (*Arrangements to safeguard and promote welfare*): <http://www.legislation.gov.uk/ukpga/2004/31/section/11>  Section 175 Education Act 2002 (*Duties of LEAs and governing bodies in relation to welfare of children*): <http://www.legislation.gov.uk/ukpga/2002/32/section/175> |

* Both parties to this arrangement will respond to any notices from the Information Commissioner that impose requirements to cease or change the way in which data is processed.
* Both parties will comply with right of access requests in compliance with the relevant legislation (GDPR/DPA), and if it is to be answered jointly to inform the MPS as soon as possible on receipt in order to comply with the statutory time limit.
* The MPS reserves the right to withdraw the use of MPS data at any time.

### 6.2.1 Children Act 2004

Section 10 of the Children Act 2004 is a statutory requirement for responsible agencies including the police to work together to ensure that children and young people are able to achieve 5 key outcomes; Be Healthy, Stay Safe, Enjoy And Achieve, Make A Positive Contribution and Achieve Economic Well Being. Section 11 places a further responsibility on listed authorities to ensure that their functions are discharged having regard to the need to safeguard and promote the welfare of children.

The sharing of data under this agreement will help the MPS to fulfil their obligations under this piece of legislation.

|  |
| --- |
| **RELEVANT LEGISLATION**  Section 10 Children Act 2004 (*Co-operation to improve well-being*): <http://www.legislation.gov.uk/ukpga/2004/31/section/10> |

### 6.2.2 Education Act 2002

Section 175 of the Education Act 2002 places a similar responsibility on Local Education Authorities and governing bodies to carry out their function with a view to safeguarding and promoting the welfare of children.

The sharing of data under this agreement will help educational establishments to fulfil their obligations under this piece of legislation.

|  |
| --- |
| **RELEVANT LEGISLATION**  Section 175 Education Act 2002 (*Duties of LEAs and governing bodies in relation to welfare of children*): <http://www.legislation.gov.uk/ukpga/2002/32/section/175> |

### 6.2.3 Common Law

In exceptional circumstances where police need to share personal data with education establishments for a policing purpose that is not directly linked to the welfare of children then a Common Law Policing Purpose will be used.

The Code of Practice on the Management of Police Information (MoPI) defines policing purposes as:

* Protecting life and property;
* Preserving order;
* Preventing the commission of offences;
* Bringing offenders to Justice;
* Any duty or responsibility arising from common or statute law.

The policing purposes supported by this data sharing activity are “P*rotecting life and property; preserving order; preventing the commission of offences and bringing offenders to justice*”.

In the sharing of victim personal data, Common Law in conjunction with consent is required to meet the processing conditions of the Data Protection Act 2018.

|  |
| --- |
| **RELEVANT LEGISLATION**  College of Policing (2014) Management of Police Information: [https://www.app.college.police.uk/app-content/data-management/management-of-police-data/](https://www.app.college.police.uk/app-content/information-management/management-of-police-information/) |

### 6.2.4 Duty of Confidence

If the service has received any data in confidence, there is almost certainly a Duty of Confidence towards the data subject.

#### 6.2.4.1 How a duty of confidence might be overridden

There is an expectation when an individual reports a crime to the police that the police will use and, if necessary, share some of that data in an appropriate and proportionate manner necessary to investigate that crime or reduce crime generally.

An obligation of confidence is not absolute and can be overridden by several factors, such as another legal obligation, the consent of the individual concerned, or by demonstrating that to disclose the data would be in the public interest.

Public interest factors for this agreement are:

* Safeguarding children
* Protecting other vulnerable people
* Preventing the commission of criminal offences
* Bringing offenders to justice

Through this data sharing agreement non-conviction or “soft” intelligence will be shared where there is real evidence of a pressing need to do so for the public interest factors already identified. Other factors informing the decision will be;

* Police belief in the truth of the allegation / data
* The interest of the third party in obtaining the data
* The degree of risk posed by the person if the disclosure (about them) is not made

### 6.2.5 Fair Processing

When data is obtained from data subjects by the MPS, they must, so far as practicable, be provided with, or have made readily available to them, the following data:

* The identity of the data controller
* If the data controller has nominated a representative for the purposes of the Act, the identity of that representative
* The purpose or purposes for which the data are intended to be processed
* Any further data which is necessary, taking into account the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

A Fair Processing Notice, covering the points specified above, can be found within police station front offices and custody suites and is published on the MPS website www.met.police.uk

#### 6.2.5.1 Exemption under Schedule 1, Part 2, Section 10(1)(2)(3) Data Protection Act 2018

This arrangement relates to the prevention or detection of crime/the apprehension or prosecution of offenders, it may operate under the exemption made available by Schedule 1, Part 2, Section 10(1)(2)(3) Data Protection Act 2018 it removes the need to apply the fair processing conditions described above. The exemption applies:

* To comply with the fair processing conditions would be likely to prejudice the purposes of the prevention or detection of crime and/or the apprehension and prosecution of offenders

Educational establishments should make their pupils generally aware of how they intend to use data provided to them, but can apply this exemption when sharing specific data with the police for the prevention or detection of crime / apprehension of offenders.

|  |
| --- |
| **RELEVANT LEGISLATION**  Schedule 1, Part 2, Section Part 2, Section 10((1)(2)(3): <http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/paragraph/10/enacted>  Section 11(1)(2: <http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/paragraph/11/enacted>  Section 18(1)(2)(3)(4) Data Protection Act 2018: <http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/paragraph/18/enacted> |

### 6.2.6 Legitimate Expectation

An individual’s expectation as to how data given to a public body will be used will be relevant in determining whether the first data protection principle has been complied with.

This data sharing agreement is consistent with the legitimate expectations of providers of data to the MPS in that the data will be used for legitimate policing purposes. In this agreement the policing purposes are working in partnership to satisfy the provisions within the Children Act 2004.

Educational establishments within London have all made their pupils aware of how their personal data is used by them and that sharing with the police may occur if it is felt that the police need to be aware of data on public safety grounds.

This data sharing agreement will be published on the MPS Publication Scheme so that members of the public can see what is done with “their” data.

### 6.2.7 Human Rights - Article 8: The right to respect for private and family life, home And correspondence

*There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society, in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*.

Article 8(1) rights are not absolute and should be weighed against the public interest, which may justify an interference with those rights. In conducting what is a balancing exercise between the rights of the individual and the interests and the good of the public at large, the Human Rights Act states the data sharing activity must be:

* In pursuit of a legitimate aim - fulfilling the purposes of The Children Act 2004 and the Education Act 2002 statute laws are the legitimate aims of this agreement.
* Proportionate - the data sharing will be proportionate on a case by case basis and in compliance with the Data Protection Act 2018.
* Appropriate and necessary to a democratic society - the purposes of The Children Act 2004 and Education Act 2002, to protect children, are necessary in a democratic society.

The vast majority of students that attend the education establishment in the London are law-abiding citizens who are developing themselves educationally for either personal or financial reasons. Crime/violent attacks, and any retaliation that may follow, could easily lead to a student receiving grievous or fatal injuries. The obvious citizen benefit is that the sharing of this data will enable the education establishment to manage the risk of students that are known to be linked with crime.

The sharing of this data is the only way to achieve the stated objectives and the personal data used is the minimum necessary to achieve the purpose and no more, and is proportionate.

Supporting law and order and working to improve its effectiveness and the public confidence in it is an activity necessary in a democratic society.

|  |
| --- |
| **RELEVANT LEGISLATION**  Article 8 Human Rights Act 1998 (*Right to respect for private and family life*): [http://www.legislation.gov.uk/ukpga/2018/42/schedule/1/part/I/chapter/7](http://www.legislation.gov.uk/ukpga/1998/42/schedule/1/part/I/chapter/7)  Children Act 2004 (*contents*): <http://www.legislation.gov.uk/ukpga/2004/31/contents>  Education Act 2002 (*contents*): <http://www.legislation.gov.uk/ukpga/2002/32/contents>  Data Protection Act 2018 (*contents*): <http://www.legislation.gov.uk/ukpga/2018/12/contents> |

### 6.2.8 Schedule 8, Part 3 Data Protection Act 2018

If the data is “special category data” (that is, where it relates to race, ethnic origin, political opinions, religion or belief system, membership of a trades union, physical/mental health or sexual life, the commission or alleged commission of any offence, proceedings relating to the offence) you must also satisfy at least one condition in Schedule 3.

The sharing of special category data in this agreement satisfies the following conditions of Schedule 8, Part 3.

* The data subject has given his explicit consent to the processing of the personal data [1]

This will be the relevant condition where consent has been sought from a victim or a witness to share data with their school for their benefit.

**or**

* The processing is necessary for the exercise of any enactment [7(b)]
* The enactment for this data sharing agreement which makes this condition relevant is S.11 Children Act 2004 and S. 175 Educational Act 2002.

**or**

* The personal data are processed in circumstances specified in an order made by the secretary of state. [10]

These circumstances are defined in Statutory Instrument 417/2000 - The Data Protection (Processing of Sensitive Personal Data) Order 2000, which provides for sensitive personal data being processed where:

“The processing is necessary for the exercise of any functions conferred on a constable by any rule of law.” (Paragraph10).

The explanatory notes attached to the Order state that this might be used where a Common Law power is the legal basis to share personal sensitive data.

|  |
| --- |
| **RELEVANT LEGISLATION**  Schedule 3 Data Protection Act 2018 (*Conditions relevant for purposes of the first principle: processing of sensitive personal data*): <http://www.legislation.gov.uk/ukpga/2018/12/section/35/enacted>  417 The Data Protection (Processing of Sensitive Personal Data) Order 2000: <http://www.legislation.gov.uk/uksi/2000/417/contents/made>  Section 11 Children Act 2004 (*Arrangements to safeguard and promote welfare*): <http://www.legislation.gov.uk/ukpga/2004/31/section/11>  Section 175 Education Act 2002 (*Duties of LEAs and governing bodies in relation to welfare of children*): <http://www.legislation.gov.uk/ukpga/2002/32/section/175> |

## 6.3 Second Principle – Data protection

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

|  |
| --- |
| Schedule 1, Part 2 Data Protection Act 2018 (*The second principle*): <http://www.legislation.gov.uk/ukpga/2018/12/section/36/enacted> |

### 6.3.1 How the agreement complies with the second data principle

The sharing of the personal data with the education establishment is to achieve the intended objectives described and is not contradictory with the purpose for which it was originally obtained by the MPS. The MPS is registered under the DPA for “Policing” and “Ancillary Support for Policing”. The data was obtained for policing purposes. Under this arrangement it will not be processed in any manner contradictory to that purpose.

## 6.4 Third Principle – Data Protection

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

|  |
| --- |
| **RELEVANT LEGISLATION**  Schedule 1, Part 2 Data Protection Act 2018 (*The third principle*): <http://www.legislation.gov.uk/ukpga/2018/12/section/37/enacted> |

### 6.4.1 How the agreement complies with the third data principle

The data to be shared with the education establishment will be the minimum necessary for both parties to conduct an accurate risk assessment and decide upon the measures required to manage an individual or provide assistance to them.

## 6.5 Fourth Principle – Data protection

Personal data shall be accurate and, where necessary, kept up to date.

|  |
| --- |
| **RELEVANT LEGISLATION**  Schedule 1, Part 2 Data Protection Act 2018 (*The fourth principle*): <http://www.legislation.gov.uk/ukpga/2018/12/section/38/enacted> |

### 6.5.1 How the agreement complies with the fourth data principle

The data to be shared will be collated from a number of MPS corporate systems and the Police National Computer. The data is therefore subject to considerable cross-checking and is subject to our normal procedures and validations intended to ensure data quality. Any inaccuracies identified by the education establishment in processing this data should be notified to the MPS for verification and, if necessary, rectification of any relevant database.

The education establishment will have no responsibility for updating, or otherwise maintaining the shared data.

## 6.6 Fifth Principle – Data Protection

Personal data shall not be stored in a form that identifies data subjects for longer than is necessary

|  |
| --- |
| **RELEVANT LEGISLATION**  Schedule 1, Part 2 Data Protection Act 2018 (*The fifth principle*): <http://www.legislation.gov.uk/ukpga/2018/12/section/39/enacted> |

### 6.6.1 How the agreement complies with the fifth data principle

Data that is shared by the Police and received the education establishment will be recorded and stored in accordance with the Management of Police Information Act 2006 (MoPI). A record of the data disclosed by the MPS should be made on crimint as part of this agreement and will include:

* who disclosed the data,
* what data was disclosed,
* the reason for the disclosure

When personal data is disclosed relating to a subject who has an existing record, this record will be updated to record the data sharing through this agreement.

MPS data processed through this agreement will be held until the subject is no longer in the education system before a review, in accordance with MoPI.

## 6.7 Sixth Principle – Data protection

Personal data shall be processed in a manner that ensures the appropriate security of the personal data.

|  |
| --- |
| **RELEVANT LEGISLATION**  Schedule 1, Part 2 Data Protection Act 2018 (*The sixth principle*): <http://www.legislation.gov.uk/ukpga/2018/12/section/40/enacted> |

### 6.7.1 How the agreement complies with the sixth data principle

The parties to this agreement must process personal data in a manner that ensures appropriate security of the personal data.

Appropriate technical and organisational measures will be put in place to guard against unauthorised or unlawful processing and against accidental loss, destruction or damage.

It is recognised that the MPS reserves the right to withdraw the right to use the data at any time.

## 6.8 Freedom of Information Act and Right of Access Requests

Normal practice will be to make all data sharing agreements available on the MPS Publication Scheme. It is recognised that parties to this agreement may receive a request for data made under the Act that relates to the operation of this agreement. Where applicable, they will observe the Code of Practice made under Section 45 of the Freedom of Information Act 2000.

This Code of Practice contains provisions relating to consultation with others who are likely to be affected by the disclosure (or non-disclosure) of the data requested. The Code also relates to the process by which one authority may also transfer all or part of a request to another authority if it relates to data held only by the other authority.

Individuals can request a copy of all the data an organisation holds on them, by making a Right of Access Request (ROAR). This may include data that was disclosed to that organisation under this agreement. Where this is the case, as a matter of good practice, the organisation will liaise with the originating organisation to ensure that the release of the data to the individual will not prejudice any ongoing investigation/prosecution.

|  |
| --- |
| **RELEVANT LEGISLATION**  Freedom of Information Act 2000: <http://www.legislation.gov.uk/ukpga/2000/36/contents>  Section 45 Freedom of Information Act 2000 (*Issue of code of practice by Secretary of State*): <http://www.legislation.gov.uk/ukpga/2000/36/section/45>  MPS Right of Access Request: [https://www.met.police.uk/globalasspublic-right-of-access-application-form](https://www.met.police.uk/globalassets/downloads/request/information/public-right-of-access-application-form.pdf) |

# 7 Agreement to abide by this arrangement

The parties signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of data between their parties in a manner compliant with their statutory and professional responsibilities.

As such, they undertake to:

* Implement and adhere to the procedures and structures set out in this agreement.
* Ensure that where these procedures are complied with, then no restriction will be placed on the sharing of data other than those specified within this agreement.
* Engage in a review of this agreement six months after its implementation and annually thereafter.

We the undersigned agree that each organisation that we represent will adopt and adhere to this data sharing agreement:

## MPS

|  |  |  |  |
| --- | --- | --- | --- |
| Post Held | Name | Signature | Date |
| Safer Schools Supervisor |  |  |  |
| Safer Schools Officer |  |  |  |

## Education Partner

|  |  |  |  |
| --- | --- | --- | --- |
| Post Held | Name | Signature | Date |
| Head Teacher /  Data Protection Officer |  |  |  |

# Appendices

## Appendix A: Data Sharing Request Form

OFFICIAL SENSITIVE

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| School details | | | | | |
| **Name** |  | | **Job Title** |  | |
| **School name** |  | | **Date** |  | |
| **Address** |  | | | | |
| **Post code** |  | | **Tel. No.** |  | |
| This request complies with GDPR and is made under sec 115 of the Crime and Disorder Act 1998(CDA), which confers on any person a power to pass information to certain relevant authorities (including police, probation, prison, health and local authorities) if necessary to help implement the provisions of that Act.  The Criminal Justice Act 2003, the Data Protection Act 1998, the European Convention on Human Rights and common law, all place a duty on the ‘responsible authority’ to share and disclose information to ensure essential and effective public protection.  I understand that any information supplied by the police is confidential in its nature and I confirm that it will be used for the specified purposes only. I undertake not to pass on any information supplied by the police to any other agency or individual without the express permission of the police. | | | | | |
| **Signed by requestor** |  | | **Date** |  | |
|  | | | | | |
| Subject requiring checks | | | | | |
| **Name** |  | | | | |
| **Date of Birth** |  | **Male  Female** | | **Ethnicity** |  |
| **Address** |  | | | | |
|  |  |  | |  | |
| Reason for request of information | | | | | |
|  | | | | | |

OFFICIAL SENSITIVE