



INFORMATION SHARING AGREEMENT

Information sharing agreement between the Metropolitan Police Service
Eastbury Community School.

Eastbury Community School



Information Sharing Agreement

ISA Ref: [1]

Protective Marking	Not Protected
Title and Version	Information sharing agreement between the Metropolitan Police Service and local schools and colleges.
Version	7.0
Purpose	Guidance document
Relevant to	Safer Schools Officers, Safer Schools supervisors, Youth Offending Teams.
Summary	An information sharing agreement between the Metropolitan Police Service and local schools and colleges for the purpose of providing a safe environment for pupils/students and staff in and around educational establishments.
Author	PC Carol-Anne O'Dwyer 784 KG
Borough	Barking and Dagenham
Organisation	Metropolitan Police Service

Information Sharing Agreement

Table of Contents

1 Purpose of the agreement 4

2 Specific Purpose for Sharing Information 6

 2.1 Reasons for Sharing Information..... 6

 2.2 MPS Benefits 7

 2.3 Partner Agency Benefits..... 7

 2.4 Citizen Benefits..... 7

 2.5 How will this information sharing arrangement further those objectives?..... 7

 2.6 Information to be shared 8

 2.7 Does the information sharing include personal data under the Data Protection Act 1998? 8

3 Description of arrangements including security matters..... 9

 3.1 Process 9

 3.2 Value of the Information..... 9

 3.3 Methods of Information Exchange..... 9

 3.4 Confidentiality and Vetting 10

 3.5 Compliance..... 10

 3.6 Movement of Information (Physically) 11

 3.7 Movement of Information (Electronically)..... 11

 3.8 Partner’s Building and Perimeter Security 11

 3.9 Storage of Papers 11

 3.10 Storage of Information on Partner’s System..... 11

 3.11 Business Continuity 11

 3.12 Security Incidents and Breaches of the Agreement..... 12

 3.13 Disposal of Electronic Information..... 12

 3.14 Disposal of Papers 12

 3.15 Review 13

4 Legal basis for sharing and what specifically will be shared 14

 4.1 First Principle – Data protection 14

 4.1.1 Data Protection Act 1998..... 14

 4.1.2 Children Act 2004 14

 4.1.3 Education Act 2002 14

 4.1.4 Common Law 15

 4.1.5 Duty of Confidence 15

 4.1.6 Fair Processing 16

 4.1.7 Legitimate Expectation 17

 4.1.8 Human Rights - Article 8: The right to respect for private and family life, home And correspondence 17

 4.1.9 Schedule 2, Data Protection Act 1998 18

Information Sharing Agreement

4.1.10 Schedule 3, Data Protection Act 1998 18

4.2 Second Principle – Data protection..... 19

 4.2.1 How the agreement complies with the second data principle..... 19

4.3 Third Principle – Data Protection 20

 4.3.1 How the agreement complies with the third data principle 20

4.4 Fourth Principle – Data protection..... 20

 4.4.1 How the agreement complies with the fourth data principle 21

4.5 Fifth Principle – Data Protection 21

 4.5.1 How the agreement complies with the fifth data principle 21

4.6 Sixth Principle – Data protection..... 21

 4.6.1 How the agreement complies with the sixth data principle 21

4.7 Seventh Principle – Data protection 22

 4.7.1 How the agreement complies with the seventh data principle 22

4.8 Eighth Principle – Data protection 22

 4.8.1 How the agreement complies with the eighth data principle..... 22

4.9 Freedom of Information Act and Subject Access Requests 22

5 Agreement to abide by this arrangement..... 24

Information Sharing Agreement

1 Purpose of the agreement

This agreement has been developed to: Head of School – Eastbury, CP Team - Eastbury

- * Define the specific purposes for which the signatory agencies have agreed to share information.
- * Describe the roles and structures that will support the exchange of information between agencies.
- * Set out the legal gateway through which the information 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.
- * Describe the security procedures necessary to ensure that compliance with responsibilities under the Data Protection Act and agency specific security requirements.
- * Describe how this arrangement will be monitored and reviewed.
- * In addition, completion of this document will ensure that the Metropolitan Police Service can meet the information sharing requirements of the Guidance on the Management of Police Information (MoPI).

The signatories to this agreement represent the following agencies/bodies:

Metropolitan Police Service -

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 information*): <http://www.legislation.gov.uk/ukpga/1998/37/section/115>

Information sharing (*Advice for practitioners providing safeguarding services to children, young people, parents and carers*): <https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice>

Human Rights Act 1998 (*contents*): <http://www.legislation.gov.uk/ukpga/1998/42/contents>

Data Protection Act 1998 (*contents*): <http://www.legislation.gov.uk/ukpga/1998/29/contents>

College of Policing (2014) Management of police information: <https://www.app.college.police.uk/app-content/information-management/management-of-police-information/>

NOT PROTECTIVELY MARKED

Information Sharing Agreement

Information Sharing Agreement

2 Specific Purpose for Sharing Information

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, including Schools, Colleges, Pupil Referral Units (PRU) and the police, need to share information and work together to protect children and young people from harm and help them achieve successful outcomes.

Through this information sharing agreement Police and Schools will work to keep pupils/students and staff safe, reduce the risk of young people getting drawn into crime or antisocial behaviour, improve the safety of the school site and surrounding area, build positive relationships between pupils/students and police, promote shared values and improve community relations generally within the school or college 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>

Information sharing (*Advice for practitioners providing safeguarding services to children, young people, parents and carers*): <https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice>

2.1 Reasons for Sharing Information

The purpose of an information sharing arrangement is to enable agencies to exchange and share information with each other. A Protocol or Agreement provides a secure framework within which the agencies can operate and exchange information 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 information.

- * To ensure that the school or college 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 school or college 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 school or college of any known anticipated violence within or surrounding their premises, or involving their student/s in order that preventive measures may be implemented.
- * To ensure that the school or college inform Police of any anticipated violence in order that preventive measures may be 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.

Information Sharing Agreement

2.2 MPS Benefits

By sharing information, 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 information and intelligence between schools, colleges 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/pupils/students at risk of offending.
- * Contributing to wider crime prevention objectives and police supporting schools as part of overall neighbourhood policing work.

2.3 Partner Agency Benefits

Schools and colleges will benefit by having up to date information on pupils/students within the criminal justice system. This will enable them to manage any risk posed to that student or any other pupils/students who may be affected. It will allow for 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 information between agencies will enable the schools and colleges to be better able to discharge their responsibilities in their role of in loco parentis, with improved standards of pupil behaviour and attendance.

2.4 Citizen Benefits

By the effective sharing of information, 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 information sharing between partners, parents and carers.

2.5 How will this information sharing arrangement further those objectives?

Sharing information between partners is essential in achieving the objectives. Without clear channels of communication, and an agreed Information Sharing Agreement, neither party will be able to manage incidents as effectively as working together.

By sharing information the schools and colleges will be better placed to effectively deal with and help pupils/students who have been arrested or who are in the Criminal Justice System.

Information Sharing Agreement

By sharing information 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.

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

2.6 Information to be shared

Safer Schools Officers must share information in order to keep young people, teachers and visitors to the school safe.

Safer Schools Officers will check daily briefings (MetBats) for any information that may be needed for school safety. MetBats 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 MetBats 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 school immediately that someone has come to police notice for committing a criminal offence and/or act of disorder to prevent it from happening again.

Information 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, information 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 information about an individual may be shared if deemed necessary. This information may include data from police crime and intelligence systems (ie name, address, DOB, bail conditions, court dates, etc.) and their history (previous related offences, pre-existing relevant intelligence).

All information shared will be recorded on CRIMINT.

Information 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.

2.7 Does the information sharing include personal data under the Data Protection Act 1998?

Yes. Partners will be sharing both personal data and sensitive personal data as defined in the Data Protection Act 1998.

Information Sharing Agreement

3 Description of arrangements including security matters.

3.1 Process

A request for information will be made in writing by completing an information sharing request form. This can be emailed or given to the safer schools officer (PC) or the MPS youth Sergeant in physical form.

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

The information gathered will be provided to the school SPOC and/or Head Teacher. All information shared must be handled according to any protective marking given to it.

A record of the personal information disclosed will be created on CRIMINT PLUS by the officer sharing the information at the time the information is supplied (or as soon as possible thereafter). This should include what was shared and the reason for sharing. Any decision not to share information should similarly be recorded along with the reasons for the decision. Where information 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.

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

All information will remain within the European Economic Area (EEA).

3.2 Value of the Information

Personal information to be shared will be security marked '**RESTRICTED**' in accordance with the Government Protective Marking System (GPMS).

RELEVANT LEGISLATION

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

3.3 Methods of Information Exchange

Information 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. If the school does not have secure email then information will be passed by hand.

The expectation is that the sharing of information 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.

Information Sharing Agreement

Physically

- * Information will be moved by a trusted person in a closed container or package.
- * Information 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 partner organisation by name or appointment (add job title).
- * If information will be stored on removable media, these will be encrypted to government standards.

Electronically

- * Protectively marked information up to the level of RESTRICTED must be transferred using secure email. (Please note, .gov.uk and nhs.uk are not secure. Examples of secure email are .pnn, .gsi, .cjsm and nhs.net). For further information 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 IAU.
- * It is prudent to use guarded speech and keep conversations short, when sharing information via telephone
- * Avoid the use of fax for transferring protectively marked information as it is not secure. If fax is the only option, follow the guidance specified in the [PMS Toolkit](#)

3.4 Confidentiality and Vetting

The Restricted information 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 RESTRICTED information 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). Partners must confirm that employees who will access shared information will have a need-to-know that information, 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>

3.5 Compliance

All partners are responsible for ensuring the security controls are implemented and staff are aware of their responsibilities under the Data Protection Act 1998 and the Children Act 2004.

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

Information Sharing Agreement

3.6 Movement of Information (Physically)

Information will be moved by a trusted person in a closed container or package.

3.7 Movement of Information (Electronically)

Information may be passed electronically by either:

- * Secure email. Please note, .gov.uk and nhs.uk are not secure. Examples of secure email are .pnn, .gsi, .cjsm and nhs.net. For further advice and information about secure email, please consult 'Secure Email Guide'

Via telephone, provided a record is subsequently made. It is prudent to use guarded speech and keep conversations short.

RELEVANT LEGISLATION

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

3.8 Partner's Building and Perimeter Security

Where **RESTRICTED** 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.

3.9 Storage of Papers

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

3.10 Storage of Information on Partner's System

Where information is being kept electronically, partners confirm that system access controls are in place (ie. username & password / keeping permissions to a minimum) to those who have a genuine "need-to-know". It has been confirmed that access to the information can be audited.

3.11 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 information cannot be transferred by the normal method, then the default mode of delivery will be via hand between the SPOCs.

Information Sharing Agreement

If the need arises for information 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.

Electronically

If information 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 information held is graded to.

Papers

If information 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 partners to this agreement may have their own security standards & protocols, where MPS information is concerned the relevant security standards set out by the GPMS for transmitting, storing and disposing information must be adhered to at all times.

3.12 Security Incidents and Breaches of the Agreement

Security breaches (including misuse of MPS information) must be reported to the MPS SPOC within 24 hours of occurring / being detected.

- * Inform the Safer Schools supervisor
- * Include details of when, where and the full circumstances of the breach

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

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

3.13 Disposal of Electronic Information

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

3.14 Disposal of Papers

Information provided 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 Restricted waste system.

Information Sharing Agreement

3.15 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/information-management/management-of-police-information/>

Information Sharing Agreement

4 Legal basis for sharing and what specifically will be shared

4.1 First Principle – Data protection

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

RELEVANT LEGISLATION

Schedule 1, Part 1 Data Protection Act 1998 (*The principles*):

<http://www.legislation.gov.uk/ukpga/1998/29/schedule/1>

Schedule 1, Part 2 Data Protection Act 1998 (*The first principle*):

<http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/part/II/crossheading/the-first-principle>

4.1.1 Data Protection Act 1998

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

RELEVANT LEGISLATION

Data Protection Act 1998 (*contents*): <http://www.legislation.gov.uk/ukpga/1998/29/contents>

4.1.2 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 information 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>

4.1.3 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 information 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*):

Information Sharing Agreement

<http://www.legislation.gov.uk/ukpga/2002/32/section/175>

4.1.4 Common Law

In exceptional circumstances where police need to share personal information with schools or colleges 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 information sharing activity are *“Protecting life and property; preserving order; preventing the commission of offences and bringing offenders to justice”*.

In the sharing of victim personal information, Common Law in conjunction with consent is required to meet the processing conditions of the Data Protection Act 1998.

RELEVANT LEGISLATION

College of Policing (2014) Management of police information: <https://www.app.college.police.uk/app-content/information-management/management-of-police-information/>

4.1.5 Duty of Confidence

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

4.1.5.1 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 information 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 information 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

Information Sharing Agreement

- * Bringing offenders to justice

Through this information 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 / information
- * The interest of the third party in obtaining the information
- * The degree of risk posed by the person if the disclosure (about them) is not made

4.1.6 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 information:

- * 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 information 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

4.1.6.1 Exemption under S.29 Data Protection Act 1998

If the purpose of the arrangement relates to the prevention or detection of crime/the apprehension or prosecution of offenders, it may operate under the exemption made available by Section 29(1) DPA 1998. This 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 information with the police for the prevention or detection of crime / apprehension of offenders.

RELEVANT LEGISLATION

Section 29 Data Protection Act 1998 (*Crime and taxation*):
<http://www.legislation.gov.uk/ukpga/1998/29/section/29>

Information Sharing Agreement

4.1.7 Legitimate Expectation

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

This information sharing agreement is consistent with the legitimate expectations of providers of information to the MPS in that the information 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 information is used by them and that sharing with the police may occur if it is felt that the police need to be aware of information on public safety grounds.

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

4.1.8 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 information 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 information sharing will be proportionate on a case by case basis and in compliance with the Data Protection Act 1998.
- * 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 schools and colleges 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 information will enable the school/college to manage the risk of students that are known to be linked with crime.

The sharing of this information is the only way to achieve the stated objectives and the personal information 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*):

Information Sharing Agreement

<http://www.legislation.gov.uk/ukpga/1998/42/schedule/1/part/1/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 1998 (*contents*): <http://www.legislation.gov.uk/ukpga/1998/29/contents>

4.1.9 Schedule 2, Data Protection Act 1998

In addition to the legal criteria set out above, the information 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 information 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 information 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 information 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 information.

RELEVANT LEGISLATION

Schedule 2 Data Protection Act 1998 (*Conditions relevant for purposes of the first principle: processing of any personal data*): <http://www.legislation.gov.uk/ukpga/1998/29/schedule/2>

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>

4.1.10 Schedule 3, Data Protection Act 1998

If the information is “sensitive” (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 sensitive personal information in this agreement satisfies the following conditions of Schedule 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 information with their school for their benefit.

Information Sharing Agreement

or

- * The processing is necessary for the exercise of any enactment [7(b)]
- * The enactment for this information 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 information 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 information.

RELEVANT LEGISLATION

Schedule 3 Data Protection Act 1998 (*Conditions relevant for purposes of the first principle: processing of sensitive personal data*): <http://www.legislation.gov.uk/ukpga/1998/29/schedule/3>

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>

4.2 Second Principle – Data protection

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

RELEVANT LEGISLATION

Schedule 1, Part 2 Data Protection Act 1998 (*The second principle*):
<http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/part/II/crossheading/the-second-principle>

4.2.1 How the agreement complies with the second data principle

The sharing of the personal information with the schools and colleges 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 information was obtained for policing purposes. Under this arrangement it will not be processed in any manner contradictory to that purpose.

Information Sharing Agreement

4.3 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.

4.3.1 How the agreement complies with the third data principle

The information to be shared with the school/college will be the minimum necessary for the college to conduct an accurate risk assessment and decide upon the measures required to manage an individual or provide assistance to them.

In pursuance of the objectives, the information 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

- * Name /alias
- * Date of birth
- * Address
- * Gender
- * Ethnicity
- * Physical description/ image

Information 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 information, for example behaviour
- * Any known risk

The Police systems that may be interrogated for information are:

- * 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 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 1998 (*The fourth principle*):

<http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/part/II/crossheading/the-fourth-principle>

Information Sharing Agreement

4.4.1 How the agreement complies with the fourth data principle

The information to be shared will be collated from a number of MPS corporate systems and the Police National Computer. The information 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 college in processing this information should be notified to the MPS for verification and, if necessary, rectification of any relevant database.

The school/college will have no responsibility for updating, or otherwise maintaining the shared information.

4.5 Fifth Principle – Data Protection

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

4.5.1 How the agreement complies with the fifth data principle

Information that is shared by the Police and received the school / college will be recorded and stored in accordance with the Management of Police Information Act 2006 (MoPI). A record of the information disclosed by the MPS as part of this agreement will include:

- * who disclosed the information,
- * what information was disclosed,
- * the reason for the disclosure

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

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

4.6 Sixth Principle – Data protection

Personal data shall be processed in accordance with the rights of data subjects under this Act.

RELEVANT LEGISLATION

Schedule 1, Part 2 Data Protection Act 1998 (*The sixth principle*):

<http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/part/II/crossheading/the-sixth-principle>

4.6.1 How the agreement complies with the sixth data principle

The partners to this agreement will respond and comply with any notices from the Information Commissioner that impose requirements to cease or change the way data is processed.

Any subject access requests will be dealt with in accordance with the provisions of this Act. Additionally the provider of the data will be consulted, where practicable, before the disclosure has taken place.

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

Information Sharing Agreement

4.7 Seventh Principle – Data protection

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

RELEVANT LEGISLATION

Schedule 1, Part 2 Data Protection Act 1998 (*The seventh principle*):

<http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/part/II/crossheading/the-seventh-principle>

4.7.1 How the agreement complies with the seventh data principle

Measures to satisfy the Seventh Principle are detailed in '3 Description of arrangements including security matters'.

4.8 Eighth Principle – Data protection

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

RELEVANT LEGISLATION

Schedule 1, Part 2 Data Protection Act 1998 (*The eighth principle*):

<http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/part/II/crossheading/the-eighth-principle>

4.8.1 How the agreement complies with the eighth data principle

The information is not intended for transfer outside the European Economic Area.

4.9 Freedom of Information Act and Subject Access Requests

Normal practice will be to make all information sharing agreements available on the MPS Publication Scheme. It is recognised that parties to this agreement may receive a request for information 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 information 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 information held only by the other authority.

Individuals can request a copy of all the information an organisation holds on them, by making a Subject Access Request (SAR). This may include information 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 information to the individual will not prejudice any ongoing investigation/prosecution.

RELEVANT LEGISLATION

Information Sharing Agreement

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 Subject Access Request: <http://content.met.police.uk/Article/Making-a-subject-access-request/1400005855548/1400005855548>

Information Sharing Agreement

5 Agreement to abide by this arrangement

The agencies signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between their agencies 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 information other than those specified within this agreement.
- * Engage in a review of this agreement with partners six months after its implementation and annually thereafter.

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

Agency	Post Held	Name	Signature	Date