

# **GMSS Appropriate Use of Special Category Data Declaration**

**Review Date: July 2022**

## Document Control

<b>Title / Reference:</b>	Appropriate Use of Special Category Data Declaration
<b>Status:</b>	Approved
<b>Version:</b>	V1.1
<b>Date Issued / Ratified:</b>	December 2020
<b>Originator of Document and Job Role:</b>	IG Team
<b>File Classification:</b>	Official Data
<b>Retention:</b>	Life of the organisation plus 6 years (place of deposit)
<b>Target Audience:</b>	All GMSS staff & 3 <sup>rd</sup> party partners
<b>Links to other strategies, policies, procedures etc:</b>	<ul style="list-style-type: none"> <li>• Data Security, Protection &amp; Confidentiality Policy</li> <li>• Data Security, Protection &amp; Confidentiality Framework</li> <li>• Confidentiality Audit Procedure</li> <li>• Data Security Breach &amp; Incident Reporting Policy</li> <li>• Secure Transfer of Data Policy</li> <li>• Acceptable Use of IT / Information Systems Policy</li> <li>• Information Classification Policy</li> <li>• Records Management Policy</li> <li>• Risk Management Policy</li> <li>• Information Risk Policy</li> <li>• Subject Access Request Policy</li> <li>• Registration Authority (Smart Card) Procedure</li> <li>• Data Security, Protection &amp; Confidentiality Staff Handbook</li> </ul> <p><b>This list is not exhaustive</b></p>

## Change History

Summary of Changes	Name	Date	Version
Draft – New Policy	IG Team	Jan 20	0.1
Changes made following IG Group recommendations	IG Team	Jun 20	0.2
Changes made following IG Group recommendations	IG Team	Jun 20	0.3
Changes made to content	Caldicott Guardian	Aug 20	0.4
Changes made in line with Governance Committee comments	IG Team	Nov 20	1.1

## Review

Name	Role	Date	Version
IG Team	IG Team	Jan 20	0.1
IG Group	IG Group	Jan 20	0.1
IG Team	IG Team	Jun 20	0.2
IG Group	IG Group	July 20	0.2
IG Team	IG Team	July 20	0.3

IG Group	IG Group	July 20	0.3
IG Group	IG Group	Aug 20	0.4
IG Group	IG Group	Nov 20	1.1

### Approval

Name	Role	Date	Version
IG Group	IG Group	Nov 20	1.1
Governance Committee	Governance Committee	Dec 20	1.1
Senior Management Team	Senior Management Team	Dec 20	1.1

### Distribution

Name	Role	Date	Version
Updated policy tracker			
Saved in policy folder			
GMSS Publication scheme			
The Bulletin			
People Matters			

### DOCUMENT STATUS:

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled

## **Contents**

1. Introduction & Purpose .....	5
2. Definitions.....	5
3. What types of processing is undertaken by GMSS that requires an Appropriate Policy Document? .....	6
4. Lawful basis for processing.....	6
5. Procedures for securing compliance .....	6
6. Retention and Erasure of Personal Data.....	10
7. Staff Awareness.....	11
8. Classification and Retention of Information .....	11
9. Legislation & Guidelines .....	11
10. Equality Statement.....	12
11. Monitoring and Review .....	12
Appendix A.....	13

## **1. Introduction & Purpose**

This Greater Manchester Shared Services (GMSS) Appropriate Use of Special Category Data Declaration will demonstrate how GMSS will protect both Special Category and Criminal Offence data. GMSS will have a duty to ensure that the contents of this declaration are adhered to by the organisation, and the measures by which it will fulfil these are contained within this declaration.

## **2. Definitions**

### **Special Category Data**

Please find below a summary of what is meant by Special Category Data:

Article 9 of the General Data Protection Regulation (GDPR) refers to “special categories of personal data”. This data is sensitive so needs more protection. These special categories of data are:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Physical or mental health data;
- Sexual life / sexual orientation;
- Genetic data;
- Biometric data.

### **Criminal Offence Data**

The GDPR gives extra protection to “personal data relating to criminal convictions and offences or related security measures”. We refer to this as criminal offence data. This covers a wide range of information about:

- Criminal activity;
- Allegations;
- Investigations; and
- Proceedings.

It includes not just data which is obviously about a specific criminal conviction or trial, but also any other personal data relating to criminal convictions and offences, including:

- Unproven allegations;
- Information relating to the absence of convictions; and
- Personal data of victims and witnesses of crime.

It also covers a wide range of related security measures, including:

- Personal data about penalties;
- Conditions or restrictions placed on an individual as part of the criminal justice process; or
- Civil measures which may lead to a criminal penalty if not adhered to.

Please Note: Due to the nature of GMSS business, criminal offence data will only apply to any convictions declared during any employment checks or any convictions

declared during current employment. This is managed through Human Resources policies and procedures.

### **3. What types of processing is undertaken by GMSS that requires an Appropriate Policy Document?**

This declaration sets out how GMSS will protect personal, special category and criminal offence data. This declaration meets the requirement of Schedule 1 of the Data Protection Act (DPA) 2018 that organisations must have an appropriate policy document where processing of special category and criminal offence data is taking place.

This is necessary in connection with employment, social security or social protection for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the data controller/processor or the data subject.

### **4. Lawful basis for processing**

Under the GDPR, GMSS has a lawful basis for the processing of Special Category and Criminal Offence data. This refers to requirements under enactment which means that GMSS is obliged to collect and process this data. Similarly, processing of this type of data is undertaken because there is a substantial public interest in processing this information as set out under the DPA 2018.

### **5. Procedures for securing compliance**

Article 5 of the GDPR describes the data protection principles. Below sets out details on how GMSS will comply with these in relation to the processing of Special Category and Criminal Offence data.

#### **Principle 1 – Fair, Lawful and Transparent**

Special Category and Criminal Offence data is processed lawfully, fairly and in a transparent manner in relation to the data subject.

The following will be undertaken by GMSS to ensure compliance of Principle 1:

- GMSS will ensure that personal, special category and criminal offence data is only processed where a lawful basis applies and where processing is otherwise lawful;
- GMSS will only process personal, special category and criminal offence data fairly and will ensure that data subjects are not misled about the purposes of any processing; and
- GMSS will ensure that data subjects receive full privacy information so that any processing of personal, special category and criminal offence data is transparent via Privacy Notices.

The following outlines how GMSS demonstrates compliance of Principle 1:

- The Data Security Protection & Confidentiality Policy outlines how GMSS will process personal and special category data which the organisation will adhere to.
- All data processed is assessed in line with the Information Risk Policy and all findings are documented in the organisations Information Asset Registers, this includes the legal basis for processing.
- Privacy Notices documenting the purpose of processing and full privacy

information are made readily available to data subjects via the GMSS website or directly from the GMSS IG Team if requested.

- Due to the nature of GMSS business, criminal offence data will only apply to any convictions declared during any employment checks or any convictions declared during current employment. This is managed through the organisations Human Resource's policies and procedures.

## **Principle 2 – Fit for Purpose**

Special Category and Criminal Offence data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The following will be undertaken by GMSS to ensure compliance of Principle 2:

- GMSS will only collect personal, special category and criminal offence data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a Privacy Notice;
- GMSS will not use personal, special category and criminal offence data for purposes that are incompatible with the purposes for which it was collected. If we do use personal, special category and criminal offence data for a new purpose that is compatible we will inform the data subject first.

The following outlines how GMSS demonstrates compliance of Principle 2:

- The Data Security Protection & Confidentiality Policy outlines how GMSS will process personal and special category data which the organisation will adhere to.
- All processing purposes are documented in the organisations Information Asset Registers.
- Privacy Notices documenting the purpose of processing and full privacy information are made readily available to data subjects via the GMSS website or directly from the GMSS IG Team if requested.
- Due to the nature of GMSS business, criminal offence data will only apply to any convictions declared during any employment checks or any convictions declared during current employment. This is managed through the organisations Human Resource's policies and procedures.

## **Principle 3 – Adequate and Relevant**

Special Category and Criminal Offence data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are being processed.

The following will be undertaken by GMSS to ensure compliance of Principle 3:

- GMSS will only collect the minimum personal, special category and criminal offence data that we need for the purpose for which it is collected. We will ensure that the data we collect is both adequate and relevant.

The following outlines how GMSS demonstrates compliance of Principle 3:

- The Data Security Protection & Confidentiality Policy outlines how GMSS will process personal and special category data which the organisation will adhere to.
- The Records Management Policy which the organisation will adhere to,

outlines that all data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed. This is documented in the organisations Information Asset Registers and Data Flow Mapping Registers.

- Privacy Notices documenting the purpose of processing and full privacy information are made readily available to data subjects via the GMSS website or directly from the GMSS IG Team if requested.
- Due to the nature of GMSS business, criminal offence data will only apply to any convictions declared during any employment checks or any convictions declared during current employment. This is managed through the organisations Human Resource's policies and procedures.

#### **Principle 4 – Accuracy**

Special Category and Criminal Offence data is accurate and, where necessary, kept up to date.

The following will be undertaken by GMSS to ensure compliance of Principle 4:

- GMSS will ensure that personal, special category and criminal offence data is accurate and kept up to date where necessary. We take particular care to do this where our use of the personal, special category and criminal offence data has a significant impact on individuals.

The following outlines how GMSS demonstrates compliance of Principle 4:

- The Data Security Protection & Confidentiality Policy outlines how GMSS will process personal and special category data which the organisation will adhere to.
- The Records Management Policy which the organisation will adhere to, outlines that all data must be accurate and kept up to date. This is documented in the organisations Information Asset Registers and Data Flow Mapping Registers.
- Privacy Notices documenting the purpose of processing and full privacy information are made readily available to data subjects via the GMSS website or directly from the GMSS IG Team if requested.
- Due to the nature of GMSS business, criminal offence data will only apply to any convictions declared during any employment checks or any convictions declared during current employment. This is managed through the organisations Human Resource's policies and procedures.

#### **Principle 5 – Data Retention**

Special Category and Criminal Offence data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

The following will be undertaken by GMSS to ensure compliance of Principle 5:

- GMSS will only keep personal, special category and criminal offence data in an identifiable form for as long as it is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal, special category and criminal offence data, it will be deleted or rendered permanently anonymous. At all times GMSS will follow the Records Management Code of Practice for Health and Social Care 2016 (NHS Digital).



The following outlines how GMSS demonstrates compliance of Principle 5:

- The Data Security Protection & Confidentiality Policy outlines how GMSS will process personal and special category data which the organisation will adhere to.
- The Records Management Policy which the organisation will adhere to, outlines GMSS's Retention Schedule which includes special category and criminal offence data. As part of the records management process, the organisation will follow the Retention of Information Procedure.
- The Information Asset Registers and Data Flow Mapping Registers document the retention periods.
- Privacy Notices documenting the purpose of processing and full privacy information are made readily available to data subjects via the GMSS website or directly from the GMSS IG Team if requested.
- Due to the nature of GMSS business, criminal offence data will only apply to any convictions declared during any employment checks or any convictions declared during current employment. This is managed through the organisations Human Resource's policies and procedures.

### **Principle 6 – Security**

Special Category and Criminal Offence data is processed in a manner that ensures appropriate security of the data including: protection against unauthorised or unlawful processing; against accidental loss, destruction or damage; and by using appropriate technical or organisational measures.

The following will be undertaken by GMSS to ensure compliance of Principle 6:

- GMSS will at all times have appropriate organisational and technical measures in place to protect personal, special category and criminal offence data.

The following outlines how GMSS demonstrates compliance of Principle 6:

- The Information Security Policy, Acceptable Use of IT / Information Systems Policy and Secure Transfer of Data Policy outlines how GMSS will protect personal and special category data and details technical measures which the organisation will adhere to.
- The Information Asset Registers and Data Flow Mapping Registers document the organisational and technical measures which are in place to protect the data.
- Mandatory Data Protection Impact Assessments will be carried out, as and when new / amendments to systems and processes are made within the organisation in order to protect and highlight any risks to personal, special category and criminal offence data.
- GMSS IT provide assurances via compliance with Cyber Essentials Plus accreditation and ISO27001 and evidence to support the Data Security and Protection Toolkit (DSPT).
- Privacy Notices documenting the purpose of processing and full privacy information are made readily available to data subjects via the GMSS website or directly from the GMSS IG Team if requested.
- Due to the nature of GMSS business, criminal offence data will only apply to any convictions declared during any employment checks or any convictions declared during current employment. This is managed through the

organisations Human Resource's policies and procedures.

## **Principle 7 - Accountability**

GMSS is responsible for and will demonstrate compliance with these 6 principles. Our Data Protection Officer (DPO) is responsible for monitoring GMSS's compliance with these principles.

The following will be undertaken by GMSS to ensure compliance of Principle 7:

- GMSS will ensure that records are kept of all personal, special category and criminal offence data processing activities (ROPA) and that these are provided to the Information Commissioner on request – please see the Information Asset Register and Data Flow Mapping Register;
- GMSS will carry out Data Protection Impact Assessments for any high-risk personal, special category and criminal offence data processing, and consult the Information Commissioner if appropriate;
- GMSS has a Data Protection Officer appointed, who is the IG Manager, to provide independent advice and monitoring of GMSS's personal, special category and criminal offence data processing and has access to report to the highest management level in GMSS;
- GMSS will at all times be able to demonstrate that it has robust internal processes in place to ensure that personal, special category and criminal offence data is only collected, used or handled in a way that is compliant with data protection law. Please see the Data Security / Information Governance policies, procedures and templates.

The following outlines how GMSS demonstrates compliance of Principle 7:

- The Data Security & Protection Framework and the Data Security Protection & Confidentiality Policy outlines how GMSS will process personal and special category data which the organisation will adhere to.
- Mandatory Data Protection Impact Assessments will be carried out, as and when new / amendments to systems and processes are made within the organisation in order to protect and highlight any risks to personal, special category and criminal offence data.
- The DPO provides updates through the IG Group, Governance Committee and Senior Management Team on a regular basis on all DPO elements.
- All data processed is assessed in line with the Information Risk Policy and all findings are documented in the organisations Information Asset Registers and Data Flow Mapping Registers.
- The organisation has a suite of Data Security & Protection (IG) Policies and Procedures in line with the DSPT. Please see Appendix A for a full list of available Policies and Procedures.
- Privacy Notices documenting the purpose of processing and full privacy information are made readily available to data subjects via the GMSS website or directly from the GMSS IG Team if requested.
- Due to the nature of GMSS business, criminal offence data will only apply to any convictions declared during any employment checks or any convictions declared during current employment. This is managed through the organisations Human Resource's policies and procedures.

## **6. Retention and Erasure of Personal Data**

GMSS has a legal responsibility to ensure that personal, special category and criminal offence data is retained and erased in line with the Records Management Policy.

The following will be undertaken by GMSS to ensure compliance of the above:

- GMSS will have a record of processing activities (ROPA). This includes, where possible, the envisaged time limits for erasure of the different categories of data;
- Where GMSS no longer requires personal, special category and criminal offence data for the purpose for which it was collected, GMSS will follow confidential waste and / or archiving processes – please see the Records Management Policy for further information;
- GMSS will at all times ensure that individuals, both public and staff receive full privacy information (Privacy Notices) about how their data is processed and this will include the period for which the personal, special category and criminal offence data will be stored, or if that is not possible, the criteria used to determine that period.

The following outlines how GMSS demonstrates compliance of the above:

- The Records Management Policy which the organisation will adhere to, outlines GMSS's Retention Schedule which includes retention periods, archiving and erasure procedures for personal, special category and criminal offence data. As part of the records management process, the organisation will follow the Retention of Information Procedure.
- The Information Asset Registers and Data Flow Mapping Registers document the retention periods.
- Privacy Notices documenting the purpose of processing and full privacy information are made readily available to data subjects via the GMSS website or directly from the GMSS IG Team if requested.
- Due to the nature of GMSS business, criminal offence data will only apply to any convictions declared during any employment checks or any convictions declared during current employment. This is managed through the organisations Human Resource's policies and procedures.

## **7. Staff Awareness**

This declaration will be made available to all staff via The Bulletin and published on Publication Scheme.

All staff are responsible for adhering to the General Data Protection Regulations 2018, Caldicott Principles, the National Data Guardian Data Security Standards, the Data Protection Act 2018 and the Common Law Duty of Confidentiality.

All staff must be aware of the content and location of this declaration. If staff have any queries regarding this declaration, they must in the first instance contact the IG Team.

## **8. Classification and Retention of Information**

GMSS will continue to implement appropriate information classifications controls, based upon the data security legislation.

Further details of the classifications controls can be found in the Information Classification Policy and the Records Management Policy.

## **9. Legislation & Guidelines**

A set of procedural documents will be made available via People Matters.

- General Data Protection Regulations 2016
- Data Protection Act 2018
- The National Data Guardian Data Security Standards
- Confidentiality: NHS Code of Practice
- Common Law Duty of Confidence
- Human Rights Act 1998
- Computer Misuse 1998
- Electronic Communications Act 2000
- Guide to the Notification of Data Security and Protection Incidents.

## **10. Equality Statement**

GMSS aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this declaration and its impact on staff, patients and the public have been reviewed in line with the GMSS legal equality duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/belief.

The Equality Analysis has been completed and any associated policies and procedures will be analysed accordingly.

## **11. Monitoring and Review**

This declaration will be monitored through staff awareness and supporting evidence to the Data Security & Protection Toolkit.

This declaration will be reviewed on a two-yearly basis and in accordance with the following as and when required:

- Legislative changes;
- Good practice guidance;
- Case law;
- Significant incidents reported;
- New vulnerabilities; and
- Changes to organisational infrastructure.

The next review is scheduled for July 2022.

## Appendix A

<b>GMSS Data Security &amp; Protection (IG) Policies &amp; Procedures</b>
<b>Policy</b>
Data Security, Protection & Confidentiality Policy (IG Policy)
Secure Transfer of Data Policy
Freedom of Information Policy
Risk Management Policy
Data Security Breach & Incident Reporting Policy
Subject Access Request Policy
Information Security Policy
Acceptable Use of IT / Information Systems Policy
Information Risk Policy
Records Management Policy
Appropriate Use of Special Category Data Declaration
Information Classification Policy
<b>Procedures</b>
Individual Rights Procedure
Confidentiality Audit Procedure
Retention of Information Procedure
Information Classification Procedure
Data Quality Procedure (embedded in the Records Management Policy)
<b>Framework</b>
Data Security & Protection Framework
<b>Privacy Notices</b>
Privacy Notice for patients & public
Privacy Notice for staff