Gravesham Borough Council
Data Breach Policy

Document Control

Organisation	Gravesham Borough Council (GBC)
Title	Data Breach Policy
Author	Gayle Jones
Filename	GBC Data Breach Policy
Owner	Data Protection Officer
Subject	Data Incidents
Protective Marking	Unclassified
Review date	October 2022

Revision History

Revision Date	Revisor	Previous Version	Reason for revision
October 2019	Gayle Jones (DPO)	-	Establish policy in line with GDPR & DPA 2018 – Version 1.2

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Senior Information Risk Officer (SIRO)	Stuart Bobby, Director (Corporate Services)	05/09/2019
Management Team	David Hughes, Chief Executive	01/10/2019

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address
All council employees who handle personal data and Elected Members	All job titles	Via NetConsent and/or email
All employees of shared services commissioned by the council who handle personal data of which GBC is the data controller.	All job titles	Via agreed process.
Publication on the council's website and staff intranet	N/A	Via Digital Team

Contributors

Development of this policy was assisted through information provided by the following organisations:

- Kent County Council

Contents

1 Objectives

1.1 Any information that could identify a living individual (directly or indirectly) is classed as personal data. GBC is required, under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18), to implement appropriate technical and organisational measures that ensures the appropriate security of the personal data it processes as the 'Data Controller'.

1.2 GBC must ensure that personal data is processed in a manner that ensures appropriate protection from unauthorised and unlawful processing and from accidental loss, destruction or damage.[1]

1.3 GBC is committed to managing personal data in a fair, transparent and lawful way.[2] It will ensure the security and integrity of information, particularly personal data and sensitive personal data by implementing and maintaining appropriate controls and procedures for its handling and storage.

1.4 Part of that commitment is to ensure that appropriate steps are taken in the event of a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

1.5 Prevention is always better than cure. Data security concerns may arise at any time and staff are encouraged to report any concerns they have to the Data Protection Officer (DPO) or the Information Governance Team (IGT). This helps GBC capture risks as they emerge, protect information and GBC from data breaches, and keep processes up-to-date and effective.

1.6 Whilst instances of the loss of personal data are rare, the consequences to GBC's reputation and the potential impact on the individuals whose data is breached (whether they are service users or employees) means that it is essential to take swift and appropriate action in the event of a data breach to:

- Contain the breach and prevent the further spread or loss, damage or destruction of data
- Recover the data that has been lost, damaged or destroyed as far as possible
- Identify risks arising from the breach
- Notify relevant parties of the breach where appropriate, and
- Prevent future breaches.

1.7 This policy sets out the steps that must be followed in the event of a data loss, theft or uncontrolled exposure of personal or sensitive information for which GBC has responsibility.

1.8 The Information Commissioner's Office (ICO) has the ability to impose significant fines of up to €20 million (euros) on data controllers for serious contraventions of the GDPR. It can also serve an enforcement notice on data controllers if it considers positive steps are necessary to bring about compliance.

2 Scope

2.1 The policy applies to all GBC staff and volunteers and, through contractual arrangements with GBC, suppliers, partners, contractors, agents, consultants and commissioned services, in the course of functions carried out for or on behalf of GBC.

[1] The sixth data protection principle, Article 5(1)(f) GDPR: 'integrity and confidentiality'

[2] The first data protection principle, Article 5(1)(a) GDPR: 'lawfulness, fairness and transparency'

2.2 Members (elected Councillors) are bound by obligations under the Members' Code of Conduct, but must also be aware of their corporate and personal responsibilities to understand the requirements of the GDPR and to act in response to any breaches in relation to personal data.

2.3 Personal data breaches may involve criminal or civil liability, or both, depending on the circumstances, and may include both individual and corporate responsibility.

2.4 Throughout this document 'information' refers to personal data or to information that is commercial or political information of a sensitive/confidential nature. GBC classifies its information according to Government policy on Protective Marking Scheme. https://www.gov.uk/government/publications/government-security-classifications

2.5 Computerised equipment, for the purposes of this policy, includes, but is not limited to personal computers (PCs – lap tops, notebooks, tablets and smartphones, application servers, file/print servers) and mobile phones. It also includes all types of removable storage media; peripheral devices and/ accessories physically attached, or connected by wireless networks, to the computerised equipment.

3 Roles and responsibilities

3.1 The Data Protection Officer (DPO) has overall responsibility for this policy. This policy will be reviewed every 3 years, or earlier if necessary.

3.2 Directorates are responsible for ensuring operational compliance with this policy within their service areas and for seeking advice from the Data Protection Officer or the Information Governance Team (IGT).

3.3 It is important that all staff are aware of their responsibilities for handling personal data, keeping it secure and not disclosing it without proper authorisation. Personal information must not be misused. Managers must ensure that staff are familiar with the appropriate policies, including the Data Protection and Information Security policies, and complete the mandatory Information Governance and GDPR training courses prior to being given access to personal data.

3.4 Anyone who handles personal or sensitive information for and/or on behalf of GBC must:

- Take all reasonable steps to ensure the security of that information to minimise the risk of a data breach, including the loss of personal or sensitive information;
- Be familiar with GBC's Data Protection and Information Security Policies;
- Follow the procedure outlined below in the event of any breach of security.

4 What is a personal data breach?

4.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. This means that a personal data breach is not limited to just losing personal data.

4.2 A personal data breach can happen in a number of ways for various reasons:

- Loss or theft of data or equipment which holds personal data e.g. laptops, tablets, USB drives, CDs or paper copies
- Equipment failure
- Inappropriate access controls allowing unauthorised use

- Human error (such as sending an email to the wrong recipient)
- Hacking, phishing or blagging (information obtained by deception)
- Unforeseen incidents such as fire or flood.

4.3 In the event of a suspected personal data or information security breach: DO NOT WAIT – ACT and REPORT ANY INCIDENTS IMMEDIATELY

4.4 It is crucial to act quickly in the event of a data breach or suspected information security incident, in order to minimise the impact of the incident and safeguard the privacy of individuals as far as possible and minimise the risk to GBC.

4.5 The initial steps that should be taken to alert managers about an incident will vary depending on whether the incident involved a member of GBC staff, a supplier or commissioned service, a service user or member of the public or an elected Member.

4.6 The flow chart at **Appendix A** and following sections of this policy set out the steps that should be followed in the event of a data breach or information security incident.

5 Action to take on discovery of the breach

5.1 If an information breach has occurred or may occur, the officer or other person concerned should:

(a) where possible, retrieve any lost equipment or papers

(b) where theft or the loss of sensitive information which could risk the safety of others is involved, report the incident to the police with all relevant details

(c) Notify their manager/a GBC member of staff as follows:

(i) Employees and contract workers should notify their line manager, or (if unavailable) the next senior manager.

(ii) Suppliers of commissioned services (sometimes referred to as 'Data Processors') should inform their GBC contract manager.

(iii) Where a data breach is reported to the customer contact centre by a member of the public, the contact centre must inform IGT, who will refer the incident to the relevant head of service.

(iv) Elected members who identify a breach relating to their role within the council (not as a representative of their ward or political party) should initially contact the head of service or director concerned.

(d) Report the loss of any IT equipment or an electronic security breach to the IT Service Desk. Where the security breach or suspected security breach involves PSN data, this must be reported to the PSN immediately via IT Services

(e) Complete a data incident report form, which can be found under the documents and forms section of the staff intranet and should be completed in liaison with the employee's line manager if necessary. (The form asks for a name, but this does not have to be given if the person concerned would prefer to report the incident anonymously).

(f) Email the completed form to gdpr@medway.gov.uk. An anonymous report can be submitted by a non-electronic method, e.g. internal post to the IG Team or the DPO.

5.2 The officer or other person should not take any further action in relation to the breach. He or she must not notify any affected individuals or regulators.

5.3 The IG team will:

(a) acknowledge receipt of the data incident report (if the person making the report has given their name);

(b) log the breach in the security incident log;

(c) notify the Chief Executive and members of Management Team of the breach and ensure they receive a copy of the data incident report.

(d) take appropriate steps to deal with the report in collaboration with the appropriate data breach team (see below).

5.4 The director or head of service must nominate an appropriate senior officer as 'breach owner' who must attend any meetings of the data breach team.

5.5 If a breach is suspected to have taken place the following information will be required in order to assess the seriousness of the breach.

(a) What type of data is involved?

(b) How sensitive is the data?

(c) Who is affected by the breach, i.e. the categories and approximate number of data subjects involved?

(d) The likely consequences of the breach on affected data subjects. e.g. what harm can come to those individuals, are there risks to physical safety or reputation, or financial loss?

(e) Where data has been lost or stolen, are there any protections in place such as encryption or pseudonymisation?

(f) What has happened to the data, e.g. if data has been stolen, could it be used for harmful purposes?

(g) What could the data tell a third party about the data subject, e.g. could the loss of apparently trivial snippets of information help a determined fraudster build up a detailed picture of other people?

(h) What are the likely or wider consequences of the personal data breach on GBC e.g. loss of reputation, loss of business, liability for fines, loss of public confidence?

6 Managing and recording the breach

6.1 On being notified of a suspected personal data breach, the breach owner will assemble an appropriate data breach team taking any necessary advice from the DPO or IGT. Where a serious breach occurs, the data breach team will be led by the DPO with the support of the IGT team (the breach owner will lead the data breach team in the event of a minor breach with support of the IGT).

6.2 Depending on the type of breach, in addition to the 'breach owner' the data breach team may compromise:

<u>Serious Breach</u>

- The DPO
- The SIRO
- The Director or head of service
- The Corporate Risk Manager
- The Corporate Information Security Officer
- The Chief Information Officer (where any breach concerns IT systems)

- The Director for HR or Head of HR
- Communications Manager
- Information Governance Team member

Minor Breach

- The head of service
- IT team member (with an understanding of the technical implications of the breach)
- Information Governance Team member
- The team leader or line manager

6.3 Responsibility rests with the Director, or their nominated deputy, to consider the action to be taken for both serious and minor breaches, to:

- Protect the interests of any individuals involved
- Secure any information lost
- Ensure the continuing delivery of the service
- Protect GBC's interests
- Meet the requirements of the GDPR/DPA18 in terms of steps to be taken under this policy

6.4 The data breach team will take immediate steps to establish whether a personal data breach has, in fact, occurred. If so, the data breach team will take appropriate action to:

- Investigate and contain the data breach and (so far as reasonably practicable) recover, rectify or delete the data that has been lost, damaged or disclosed (subject to any requirements to preserve potential evidence)
- Identify how the breach occurred and take immediate steps to stop or minimise the further loss, destruction or unauthorised disclosure of personal data
- Assess and record the breach in GBC's data breach register
- Notify appropriate parties of the breach and informing them what they must do (this could be finding lost equipment, isolating or closing part of the network or changing passwords)
- Fully assess the risk in terms of the potential adverse consequences for individuals: how serious are the consequences and how likely are they to happen?
- Take steps to prevent further breaches

7 Notifying appropriate parties of the breach

7.1 The data breach team must discuss with the DPO and IGT when they are considering whether to notify:

- The ICO
- Affected data subjects
- The Police
- The PSN (Public Service Network) team
- The NCSC (National Cyber Security Centre) (where applicable)
- Any other parties e.g. insurers or commercial partners

7.2 Ultimately the decision whether to notify lies with Directors in liaison with the DPO, particularly where the implications of the breach would seriously affect GBC's reputation. Failing to notify a breach when required to do so can result in a significant fine up to €10 million (Euros).

8 Notifying the ICO

8.1 GBC is required under the GDPR to notify the ICO[3] when a personal data breach has occurred unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. By this it means, but is not limited to:

- discrimination
- damage to reputation
- financial loss
- loss of confidentiality
- or any other significant economic or social disadvantage.

8.2 Where ICO notification is required, this shall be done without undue delay and, where feasible, not later than 72 hours after having become aware of it. Where the notification to the ICO is not made within 72 hours, it will be accompanied by reasons for the delay. The DPO/IGT team will notify the ICO on behalf of the data breach team.

8.3 If the data breach team is unsure whether or not to report, the presumption should be to report. The data breach team will take account of the factors set out at **Appendix B** and the further examples in the table at **Appendix D**.

8.4 Any notification to the ICO must[4]:

(a) Describe the nature of the personal data breach including, where possible the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.

(b) Communicate the name and contact details of the DPO or other contact who can provide information.

(c) Describe the likely consequences of the personal data breach.

(d) Describe the measures taken or proposed to be taken by GBC to address the personal data breach, including, where appropriate, measures to mitigate any possible adverse effects.

8.5 If all the information is not available within 72 hours this information may be provided in phases, provided the further information is provided to the ICO without undue delay.[5]

9 Notifying data subjects

9.1 Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data breach team will notify the affected individual(s) without undue delay[6].

9.2 The risk exists when the breach leads to physical, material or non-material damage for the individuals whose data have been breached (this could include theft, fraud, financial loss, discrimination or damage to reputation). If the breach involves personal data that reveals any of the following aspects, the damage should be considered likely to occur:

- Racial or ethnic origin
- Political opinion

[3] Article 33(1) GDPR
[4] Article 33(3)(a) – (d) GDPR
[5] Article 33(4) GDPR
[6] Article 34(1) GDPR

- Religion or philosophical belief
- Trade union membership
- Genetic data
- Health
- Sex life or sexual orientation
- Criminal convictions or offences.

9.3 Any notification must include:[7]

(a) The name and contact details of the DPO or other contact point where more information can be obtained

(b) The likely consequences of the personal data breach

(c) The measures GBC has taken or intends to take to address the personal data breach, including, where appropriate, recommendations for mitigating potential adverse effects.

9.4 When determining whether and how to notify data subjects of the breach, the data breach team will:

- Co-operate closely with the ICO (consulting it about how to inform data subjects if necessary)
- And other relevant authorities, e.g. the police
- Take account of the factors set out in the table at **Appendix C**.

9.5 In some circumstances, service users are vulnerable adults and children and being informed of a security incident may be alarming. In these circumstances the Director or their nominated deputy will consider appropriate communication strategies.

9.6 It may be important to point out at an early stage of a security incident (rather than a confirmed breach) that there is no indication that their personal security has been breached but the member of the public must remain vigilant and will be advised of any change in security status. If any of the information relates to personal finances details then the individual should be advised to contact their bank or building society urgently and to monitor their bank/building society account(s).

9.7 The Director or nominated deputy will need to authorise a briefing for all the necessary parties within a single email, blind copied (BCC) to the appropriate contacts. Depending on the potential seriousness of the security breach, contact is advised by phone as well as face to face. Any significant change to status will require follow-up communication.

10 Notifying the Police and other parties

10.1 The data breach team will already have considered whether to contact the police for the purpose of containment and recovery. Regardless of this, if it subsequently transpires that the breach arose from a criminal act perpetrated against or by a representative of GBC, the data breach team will notify the police and/or relevant law enforcement.

10.2 The data breach team will consider whether there are any legal or contractual requirements to notify any other parties, e.g. in compliance with a contract or a data sharing agreement.

[7] Article 34 (2) GDPR

11 Preventing future breaches

11.1 Once the personal data breach has been dealt with, in accordance with this plan, the data breach team will:

- Establish what security measures were in place when the breach occurred
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again
- Consider whether there is adequate staff awareness of security issues and address any gaps through training, tailored advice or capability
- Consider the outcome of any investigations into the cause of the breach and whether action should be taken under GBC's disciplinary procedure
- Consider whether it is necessary to update GBC's privacy risk assessments
- Update GBC's privacy risk register, Security Incident Log to CLOSED and Data Breach Register with the facts of the breach, its effects and the remedial action taken[8].

11.2 A security incident must remain in the 'OPEN' status, until finally resolved and only 'CLOSED' after it has been resolved, reviewed and any requirements for training, disciplinary and/or procedural changes have been identified. As well as OPEN/CLOSED it is recommended that the incident has a traffic light (Red-Amber-Green) status which is reviewed regularly, both through any information governance and directorate risk management procedures.

12 Monitoring and review

12.1 GBC will monitor the effectiveness of all its policies and procedures regularly, and conduct a full review and update as appropriate, at least annually.

12.2 GBC's monitoring and review exercises will include looking at how its policies and procedures are working in practice to reduce the risks posed to the council.

13 Staff awareness and training

13.1 Key to the success of GBC's systems is its staff awareness and understanding.

13.2 GBC provides regular training to staff:

- at induction
- on an ongoing basis as this must be refreshed every two years
- when there is any change to the law, regulation or our policy
- when significant new threats are identified
- in the event of an incident affecting the council or its service users.

14 Consequences of non-compliance

14.1 Failure to comply with this policy and associate policies (e.g. GBC's Data Protection or Information Security Policies) puts individuals and GBC at risk.

14.2 Failure to notify the DPO or IGT of an actual or suspected personal data breach is a very serious issue.

14.3 A failure to comply with this policy by:

[8] Article 33(5) GDPR

- **GBC employees:** may result in disciplinary action and may, in cases of Gross Misconduct (including negligence), result in termination of employment
- **GBC Members:** may be referred to the Standards Committee, which can recommend disciplinary measures to the Council
- **Third-Parties:** (agents, contractors and consultants) engaged to carry out work for and on behalf of Gravesham Borough Council: may result in the termination of the contract and/or litigation.

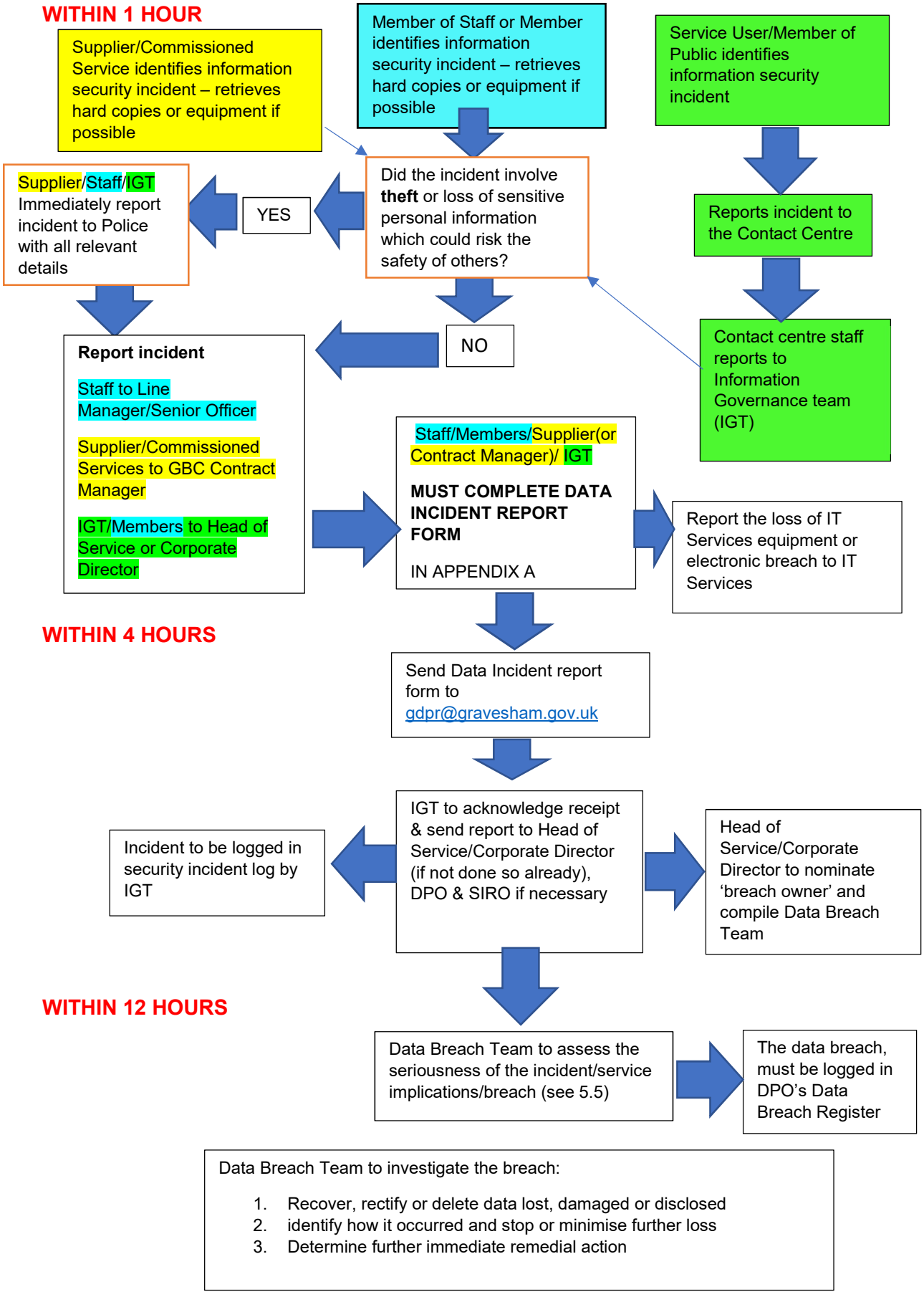
15 Definitions, assistance and guidance

15.1 Definitions and examples of Security Incidents are included in this policy at **Appendix D**.

15.2 If staff, suppliers or members do not understand this policy or if more details are needed regarding any of the steps or staff and others' responsibilities then contact GBC's:

- Data Protection Officer and Information Governance Team: gdpr@medway.gov.uk
- Advice on Information Security and Information Risk Management can be obtained by contacting the IT Services.

APPENDIX A: INFORMATION SECURITY INCIDENT REPORTING



WITHIN 48 HOURS

Data Breach Team (DBT) to consider notification to appropriate parties in liaison with the Corporate Director and DPO / IGT

DBT to consider if any legal/contractual requirements to notify other parties e.g. contract/data sharing agreement/insurance

DBT to notify police if breach arose from a criminal act if not done so already

DBT to determine if incident amounts to a personal data breach likely to result in a risk to the rights and freedoms of data subjects (see 8.1, 9.2)

If YES notify

DPO / IGT

DBT and Corporate Director to Consider appropriate communication strategies for individuals affected

If YES-notify DPO / IGT

NOTIFY the **ICO** without undue delay AND **not later than 72 hours**

DBT to co-operate with the ICO on how to inform data subjects if necessary (see Appendix B)

WITHIN 72 HOURS

DBT to ensure ICO notification includes:

1. Description of the breach, including categories and approximate number of data subjects
2. The name and contact details of the DPO or other contact for information
3. Description of the likely consequences of the breach
4. Description of the measures taken or proposed to be taken by GBC to address any breach, including measures to mitigate any possible adverse effects.

A failure to report within 72 hours will require reasons for the delay to be reported to the ICO.

NOTIFY the data subjects without undue delay

DBT to ensure notification to data subjects includes:

1. The name & contact details of the DPO or other contact for information
2. The likely consequences of the data breach
3. The measures GBC has or intends to take to address the personal data breach including, where appropriate, recommendations for mitigating potential adverse effects.

WITHIN 8 WEEKS

DBT to assess

1. Security measures in place at the time of the breach
2. Whether technical or organisational measures can be implemented to prevent another breach
3. Assess whether staff awareness or training needs to be implemented & ACTION
4. Consider if any disciplinary action is required under GBC disciplinary procedure
5. Consider if necessary to update GBC's privacy risk assessments
6. Update the Data Breach Register with the facts of the breach its effects and the remedial action taken and when appropriate update the security incident log to CLOSED

APPENDIX B: Factors for considering a report to the ICO

Factor	Explanation	Typical Example(s)/ Report to ICO?
The potential harm to the rights and freedoms of data subjects	This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. The personal data breach **must be reported** unless it is unlikely to result in a risk to data subjects' rights and freedoms.	-Exposure to identity theft through the release of non-public identifiers, e.g. passport number. **YES** -Information about the private aspects of a person's life becoming known to others, e.g. financial circumstances **YES**
The volume of personal data	There should be a presumption to report to the ICO where: —a large volume of personal data is concerned, and —there is a real risk of individuals suffering some harm It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual.	—loss of an unencrypted laptop holding names, addresses, dates of birth and National Insurance numbers of 100 individuals **YES**
		—loss of a marketing list of 100 names and addresses (or other contact details) where there is no particular sensitivity of the service being marketed **NO**
The sensitivity of data	There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress. This is most likely to be the case where the breach involves special category personal data. If the information is particularly sensitive, even a single record could trigger a report.	theft of a manual paper-based filing system (or unencrypted digital media) holding the personal data and financial records of 50 named individuals **YES**

APPENDIX C: Factors for considering a notification to data subjects

Factor	Impact on obligation to notify data subject
Whether GBC has implemented and applied (to the affected personal data) appropriate technical and organisational protection measures—in particular measures that render the personal data unintelligible to any person who is not authorised to access it, e.g. encryption.	Where such measures have been implemented, it is not necessary to notify the data subject(s).
Whether GBC has taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data subjects affected by that breach is no longer likely to materialise.	Where such measures have been implemented, it is not necessary to notify the data subject(s).
Whether it would involve disproportionate effort to notify the data subject(s).	If so, it is not necessary to notify the data subject(s)—but GBC must, instead, issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
Whether there are any legal or contractual requirements to notify the data subject?	If yes, it may be necessary to notify the data subject(s) in any event.

Assessing the likelihood and severity of the risk to the rights and freedoms of data subjects in section 9

The type of breach	The type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual's medical details have been lost, and are no longer available.
The nature, sensitivity, and volume of personal data	Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of the name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child. Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data. Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A list of customers accepting regular deliveries may not be particularly sensitive, but the same data about customers who have requested that their deliveries be stopped while on holiday would be useful information to criminals. Similarly, a small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can

	reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.
Ease of identification of individuals	An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match personal data to a particular individual, but it could still be possible. Personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Additionally, appropriately-implemented pseudonymisation (the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person) can also reduce the likelihood of individuals being identified in the event of a breach. However, pseudonymisation techniques alone cannot be regarded as making the data unintelligible.
Severity of consequences for individuals	Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.
Special characteristics of the individual	A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them.
Special characteristics of the data controller	The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.
The number of affected individuals	A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. The key is to consider the likelihood and severity of the impact on those affected.

APPENDIX D: Definitions & Example Security Incidents

'Data' is information that takes many forms and includes information printed or written on paper (including photocopies and faxes), stored electronically (e.g. on computers or networked storage, disk media, digital tape, memory cards or sticks), transmitted by post or using electronic means, images, stored negatives, prints, slides, tape or video, spoken in conversation or via telephone

'Data Controller' means a person, body or public authority which alone, or jointly with others, determines the purposes and means of the processing of personal data

'Data Processor' means a natural or legal person, public authority or body to which processes personal data on behalf of a data controller.

'**Personal data**' is information about an individual who can be identified (directly or indirectly) from that information. That individual is referred to as a 'data subject'.

'Personal data breach' A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data[9] transmitted, stored or otherwise processed – e.g. accidental loss, destruction, theft, corruption or unauthorised disclosure of personal data. Under GDPR the definition has widened to include online identifiers, location data and biometric or genetic material.

Protective Marking Scheme GBC classifies its information according to Government policy on Protective Marking: https://www.gov.uk/government/publications/government-security-classifications

'**Special Category Personal Data' (sometimes known as 'Sensitive Personal Data')** is information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

A '**Security Incident**' is awareness of the possibility or actuality of a breach of security. This can take many forms, e.g. unauthorised access to, or the loss or theft of, GBC computerised equipment; the mislaying of a client's manual case file or the inappropriate disclosure of information (verbally, in writing or electronically) to someone who has no right or need to access it.

Examples of information security incidents which would need to be reported include:

- Overhearing of confidential information;
- Unauthorised access to GBC computerised equipment;
- Loss of GBC computerised equipment.

Examples of more serious breaches which will require immediate remedial action include:

[9] Article 4(12) GDPR

- Loss of one or more confidential case files;
- Email containing personal or sensitive information sent to the wrong email address;
- Fax containing personal or sensitive information sent to wrong fax number;
- Unauthorised access to, or loss of, GBC computerised equipment containing personal or sensitive information.

Examples of the most common information security incidents

MALICIOUS

- Giving information to someone who should not have access to it – verbally, in writing or electronically
- Computer infected by a virus or similar
- Sending a sensitive email to the wrong recipient
- Receiving unsolicited mail of an offensive nature
- Finding data that has been changed by an unauthorised person
- Receiving and forwarding chain letters, including virus warnings, scam warnings and other emails which encourage the recipient to forward to others
- Unknown people asking for information which could gain them access to data e.g. a password or information about a third party

MISUSE

- Use of unapproved or unlicensed software on GBC equipment
- Accessing a computer database using someone else's authorisation (e.g. user id/password)
- Writing down your password and leaving it on display
- Printing or copying confidential information and not storing it correctly or confidentially

THEFT/LOSS

- Theft/loss of a hard copy file
- Theft/loss of GBC computer equipment

'Lost and Stolen' – applies to hard copy information as well as computerised equipment, e.g. file left in a vehicle or on public transport or stolen with car or snatched in a bag, etc. Also applies to any personal details or sensitive information passed to an unauthorised individual in any manner or overheard by an unauthorised individual during a conversation.

'Loss' – In the event of the item being knowingly lost as opposed to stolen, all of the above applies except that the Police will not report a crime and cannot issue a crime number.

Example	Notify the ICO?	Notify the data subject	Notes
GBC stored a backup of an archive of personal data encrypted on a CD. The CD is stolen during a break-in.	No	No	As long as the data are encrypted, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However, if it is later compromised, notification is required.
GBC suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data and that there was no other malware present in the system.	Yes	Only the individuals affected are notified if there is a high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the ICO must be made and the additional step of notifying other individuals if there is a high risk to them.
Personal data of 5000 customers are mistakenly sent to the wrong mailing list with 1000+ recipients	Yes	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
A direct marketing email is sent to recipients in 'to' or 'cc' field, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the ICO may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

	mailing list of a psychotherapist) or if other factors present high risks (e.g. the email contains the initial passwords).		
An individual phones to report having received a benefit letter intended for someone else. A short investigation is undertaken (i.e. completed within 24 hours) and establish with reasonable confidence that a personal data breach has occurred and it is a systemic flaw so that other individuals are or might be affected.	Yes	Only the individuals affected are notified if there is a high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the ICO must be made and the additional step taken of notifying other individuals if there is a high risk to them.