APPENDIX 3

Personal Data Breach Reporting Procedure

Date: April 2021

Version: V3.0

Document Version Control

Document Version Control	
Issue Number	Date
1.0	16 April 2021 – Considered by Information Governance Group
2.0	15 May 2021 – Considered by Information Governance Champions Group
3.0	27 July 2021 – Audit Panel for Approval

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

1. Introduction

1.1 Tameside Metropolitan Borough Council (the Council) will ensure that it reacts appropriately to any actual or suspected personal data breaches relating to electronic or paper based data systems within the custody or control of the Council or its contractual third parties.

1.2 All potential breaches, irrespective of scale, **must** be reported within the first 24 hours of knowledge using this reporting procedure to allow for mitigations to be put in place, lessons to be learned and to improve data handling procedures and the breach response process.

1.3 The UK GDPR introduces a duty on all organisations to report certain personal data breaches to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

1.4 It states organisations should ensure they have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority or the affected individuals, or both.

1.5 Organisations must also keep a record of any personal data breaches or near misses, regardless of whether they are required to notify.

2 Definitions

2.1 The following terms are used throughout this document and are defined below in Table 1.

Table 1 - Definitions

Term	Definition
Data Breach	Defined in the Data Protection Act 2018 at **s.33(3)** as "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. *The UK GDPR definition is:* A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals. Categories/Examples of breaches are provided at **Appendix 1.**
Near Miss	This is a situation where the breach has been contained without exposing any individuals to a risk of harm. Categories/Examples of near misses are provided at **Appendix 1.**
Personal Data	Is any personal data as defined by UK GDPR and the Data Protection Act 2018?

Term	Definition
	It is defined in the Data Protection Act 2018 at **s.3(2)** as "any information relating to an identified or identifiable living individual. Broadly this means any information (relating to a living individual who can be identified or identifiable, directly from the information in question, or indirectly identified from that information in combination with other information that is in the possession of the Council. The UK GDPR provides a non-exhaustive list of identifiers, including: • Name; • Identification number; • Location data; and • Online identifier (e.g. IP addresses). Personal data also applies to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living person. The Council is legally responsible for the storage, protection and use of personal data / information held by it as governed by UK GDPR and the Data Protection Act 2018.
Special Category information	This data is covered by Articles 6 and 9 of the General Data Protection Regulations. As it is more sensitive it needs more protection and consists of: • Race • ethnic origin • politics • religion • trade union membership • genetics • biometrics (where used for ID purposes) • health; • sex life; or • sexual orientation.

3 Roles and Responsibilities

3.1 All employees are responsible for the safe and secure use of Council information and systems.

3.2 All employees have a duty to report actual or suspected data breaches they are involved in and to fully support an investigation in accordance with this procedure. If an employee has a suspicion that a data breach has occurred in their own or another service area, the expectation is that they will notify the Information Governance Team who will follow up and investigate the potential breach with the appropriate service area.

3.3 The Information Governance Team will assess every reported breach for risk and severity and require return of the Personal Data Breach Form (Appendices 2 and 3) in order to carry out that assessment within 24 hours of the discovery of the breach.

3.4 Failure to report a potential breach within the first 24 hours of discovery will result in the Information Governance Team escalating non-compliance with Assistant Directors.

4 Reporting an Incident

4.1 The flowchart below summarises the stages in the process.

First knowledge of a potential breach
All breaches **must** be reported immediately to your Line Manager, who will obtain the relevant details and complete the PDB Referral Form.

First notification to Information Governance
The Line Manager will then send the completed Personal Data Breach Form (PDB01) at Appendix 2 to the Information Governance Team at information.governance@tameside.gov.uk, copying in the appropriate Assistant Director for information and to ensure the 24 hour Deadline is achieved.

Most of the questions on the PDB01 form are mandatory and it is important to provide as much detail as possible on the form to allow the Information Governance Team to make the most accurate assessment of the potential breach **within the first 24 hours of knowledge** of the breach. Information Governance can then work with the service area regarding any additional information that needs to be gathered.

Information Governance conduct initial triage
The Information Governance Team will assess the completed PDB01 form to determine the investigation process / journey and set the response timescales and commence the investigation.

5 Breach / Near Miss Investigation

5.1 Initial Response

5.1.2 The Personal Data Breach (PDB01) Form will be evaluated to identify if any immediate action is necessary in order to limit the damage from the breach and recover any losses. Mitigating actions should be undertaken by the service area at the earliest opportunity. The Information Governance Team will advise, if required, on any further mitigating actions not already undertaken. Action may also be needed to prevent another potential breach with similar circumstances whilst the investigation is taking place. This may include action taken to:

- prevent any further unauthorised access;
- secure any affected buildings (i.e. changing locks, access codes etc.);
- recover and secure any equipment or physical information;

- restore lost or damaged data by using backups; or
- prevent a further potential breach relating to the same information (e.g. an attempt to use stolen data to access accounts or services)

5.1.3 The Information Governance Team will notify any relevant persons, e.g. Legal Services.

5.2 **Investigation Process**

5.2.1 The Information Governance Team will triage / risk assess the impact of the Breach / Near Miss using the five categories listed below:-

	Action Necessary	**Timescales**
Very Low	Email to be sent to Director and Assistant Director advising of the Breach / Near Miss and to the employee and their manager advising that they are now subject to monitoring.	Form to be sent to the Information Governance Team **within 24 hours**. Timescales for investigation / outcome to be agreed thereafter
Low	Email to be sent to Director and Assistant Director advising of the Breach / Near Miss and to the employee and their manager advising that they are now subject to monitoring.	Form to be sent to the Information Governance Team **within 24 hours**. Timescales for investigation / outcome to be agreed thereafter
Medium	Email to be sent to Director and Assistant Director advising of the Breach / Near Miss and the employee is invited to a M**anagement Meeting** with their manager.	Form to be sent to the Information Governance Team **within 24 hours**. Timescales for investigation / outcome to be agreed thereafter
High	Contact HR for a decision on whether or not to proceed with Disciplinary Procedure. If not, progress as with medium rating.	Form to be sent to the Information Governance Team **within 24 hours**. Timescales for investigation / outcome to be agreed thereafter
Very High	Contact HR for a decision on whether or not to proceed with Disciplinary Procedure. Invariably this level will apply to Inappropriate Access Cases and any case that need to be reported to the ICO	Form to be sent **within 24 hours. Investigation commences immediately a**s **ICO deadline for reporting a Personal Data Breach is 72hours** (3 days) including Bank Holidays and Weekends.

5.2.2 The Information Governance Team at this stage may need to consult with other information governance specialists in the Council where appropriate before an investigation will commence. The investigation may involve the following:

- Senior Information Risk Owner (SIRO);
- Data Protection Officer / Data Controller;
- Service Director or a representative for the relevant part of the directorate;

- Line Manager of person who has caused the Breach;
- Head of Human Resources or a representative;
- Head of ICT / ICT Cyber Security Technical Specialist;
- Head of Media, Marketing and Communications or a representative;
- Facilities Management; and
- Caldicott Guardian

5.2.3 Depending on the type and seriousness of the breach, the police may be involved and the employee(s) suspended from the work place.

5.2.4 Should any employee be suspended, their IT equipment may need to be returned so it can be kept for safe storage and on occasion be used as evidence.

5.2.5 For some investigations, the Information Governance Team, with support of the Service Area where appropriate, may contact the Data Subject / Complainant to gather further information.

5.2.6 The investigation will be conducted in line with agreed protocols and all evidence and findings will be recorded in dedicated case folders held on the Information Governance Team's Shared Drive which has restricted access.

5.2.7 Depending on the type and seriousness of the potential breach, the Information Governance Team may require access to records and data involved stored on Council owned property or systems and / or on the property and systems of the Council's contractual Third Parties.

5.2.8 Once the investigation is completed, if a breach involves disciplinary or ICO involvement, a summary of the investigation will be presented to Senior Management for evaluation and signing off.

6 Evaluation

6.1 A consistent approach to dealing with all breaches / near misses must be maintained across the Council and each potential breach must be evaluated. It is important not only to evaluate the causes of the potential breach but also the effectiveness of the response to it.

6.2 The evaluation of the potential breach will include some of the following questions:

- Had the potential breach been identified as a risk prior to its occurrence?
- Did the potential breach occur despite existing measures being in place?
- Were current policies and procedures followed? If not, why not?
- In what way did the current measures prove inadequate?
- How likely is the potential breach to recur?
- Did the potential breach involve deliberate or reckless behaviour?

6.3 Assessment of Ongoing Risk

6.3.1 Any identified weaknesses or vulnerabilities must be accurately assessed in order to mitigate the ongoing risks to data / information. In order to make an assessment, the following factors will be considered:

- Type of data involved;
- Number of people that could be affected;

- The impact of the potential breach on the data subject(s) (e.g. financial implications, embarrassment, stress / mental anguish etc.);
- The likelihood or risk of any impact (as set out above) occurring to the data subject(s) on this occasion;
- Protections in place (e.g. encryption);
- Likelihood of the identified risk;
- Possible consequences for the Council's reputation; and
- Potential risks to public health or safety.

7 Actions / Outcomes

7.1 Once the investigation and the evaluation of the potential breach is concluded, if there are any identified actions to be carried out to prevent / minimise the risk of reoccurrence, they will be advised by means of an Investigation Report coupled with a Control Report approved by Senior Management which will provide recommendations for improvement. Implementation will be monitored in the service area involved or if required across the whole Council by the Information Governance Team.

7.2 **Notification**

7.2.1 Depending on the potential breach there may be legal, contractual or sector specific requirements to notify various parties. Notification may assist in security improvements and implementation, as well as risk mitigation. It will be determined and agreed by Legal Services, HR and / or Senior Management as part of the evaluation of a potential breach.

7.2.2 The following parties may need to be notified following a Breach / Near Miss:-

Party to be Notified	Considerations
Information Commissioner's Office (ICO)	• Does the potential breach involve personal data? If so: • If assessed as a breach, does the type and extent of the breach trigger notification? • Have we undertaken an initial assessment on the ICO website?
We have to notify the ICO **within 72 Hours** of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. The deadline to notify the ICO is non-negotiable, hence the need for reporting of all breaches to the Information Governance Team within 24 hours so that investigations can be conducted in a timely manner and referrals to Legal and the DPO be carried out within the ICO's timescale.	
Individuals	• Notification to the data subjects involved may be required where the breach is likely to result in a high risk to their rights and freedoms. This has to be determined by the Information Governance Team in conjunction with the Service Area / Legal on a case by

Party to be Notified	Considerations
	case basis and documented. The key consideration is that the decision to inform must not cause risk or harm to the data subject.
• **Other Agencies we may communicate with** (not an exhaustive list)	• Identity and Passport Service • Her Majesty's Revenue and Customs (HMRC) • Bank or credit card companies • Trade Unions • Social Work England • Any other professional regulatory bodies

7.3 **Disciplinary Action**

7.3.1 It may be deemed necessary to refer to HR to consider disciplinary action for any employee(s) involved in a breach, should it be rated as high / very high or there is a trend of breaches involving the same employee.

7.4 **Policy and Procedural Changes**

7.4.1 There may be a need to implement policy and procedural changes as a result of personal data breaches.

7.5 **Employee Notification and Training**

7.5.1 Where a breach is deemed and recorded as a Confirmed Breach, the Council expects that the employee(s) involved will complete their Mandatory Information Governance and Cyber Security (GDPR) training again and to provide evidence to their manager and the Information Governance Team that the training has been completed in the stipulated timescale. Failure to meet this requirement could result in disciplinary action.

7.5.2 There may be a requirement to notify employees of policy and procedural changes.

Categories of Potential Breaches **Appendix 1**

Type of Potential Breach	What Does a Breach look like?	What does a Near Miss look like? (for avoidance of doubt a near miss should still be reported to IG Team)
Data posted or faxed to incorrect recipient	1. Document(s) not retrieved or returned 2. Document(s) retrieved or returned after being opened	Document(s) retrieved unopened or returned to sender unopened. Needs to be evidenced
Data emailed to incorrect recipient	Document(s) emailed out or sensitive info in the body of the email are read by the incorrect recipient before double deletion / recall can take place. This includes emails sent to one single incorrect recipient, or emails sent through "reply all" when it is inappropriate to do so.	Evidence that email double deleted without document(s) or sensitive info in the body of the email being read and / or successfully recalled. Written evidence of double deletion needed
Theft of Laptop	Laptop stolen as a result of poor device security of user - laptop left unsecured in home, vehicle or in transit making it easier target to steal. Where sensitive documents have not been saved to a secure TMBC server i.e. docs saved on desktop. Where passwords have been stolen with laptop disabling encryption	If laptop is fully encrypted and secured (i.e. laptop turned off at time it was stolen and encrypted with bitlocker and user password) and user passwords is secure and not kept with the laptop, then may be near miss if either: 1. Laptop recovered (not accessed) shortly after theft. 2. Reported to IT immediately to remote lock / wipe the device (is this possible?)
Loss of Laptop	As above, but device lost due to negligence / accident rather than criminal involvement. Device lost in own home or TMBC secure office more likely to be recovered / found, so may be lower severity than theft of device or loss outside of office / home	If laptop is fully encrypted and secured (i.e. laptop turned off at time it was lost and encrypted with bitlocker and user password) and user passwords is secure and not kept with the laptop, then may be near miss if either: 1. Laptop recovered (not accessed). 2. Reported to IT immediately to remote lock / wipe the device (is this possible?)

Type of Potential Breach	**What Does a Breach look like?**	**What does a Near Miss look like? (for avoidance of doubt a near miss should still be reported to IG Team)**
Theft of Paperwork / physical records	Paperwork stolen as a result of poor storage / security at office, home, vehicle or other venue and / or failure to adhere to TMBC policies regarding retention & disposal. Paperwork left out on public display and not adequately secured in lockable storage. Paperwork cannot be encrypted and once stolen no measures can be taken to limit the information in the papers, so mitigations likely to be limited.	If paperwork found shortly after being reported stolen and does not contain any sensitive information. It is very unlikely there will be any cases of near miss as unable to prove whether the docs have been read and may be difficult to establish if any missing pages from the recovered docs, particularly for larger docs
Loss of Paperwork / physical records	As above, but paperwork lost due to negligence / accident rather than criminal involvement. Paperwork lost in own home or TMBC secure office more likely to be found but if found by family members or other staff could still be a breach as paperwork will not be secured from unauthorised reading.	As above. Very unlikely to be near miss unless limited personal data in the document(s) or can evidence that between loss and recovery no one else had access to the document(s)
Theft of Mobile Phone	Mobile Phone stolen as a result of poor device security of user (including password being stored with phone) - phone left unsecured in home, vehicle or in transit making it easier target to steal. If unencrypted then level of breach will be significantly worse.	Mobile Phone encrypted and theft reported to IT immediately to allow remote locking / wiping of the device. Password must have been kept away from the device and secure.
Loss of Mobile Phone	As above, but device lost due to negligence / accident rather than criminal involvement. Device lost in own home or TMBC secure office more likely to be recovered / found, so lower severity than theft of device or loss outside of office / home	Mobile Phone encrypted and loss reported to IT immediately to allow remote locking / wiping of the device. Password must have been kept away from the device and secure.

Type of Potential Breach	**What Does a Breach look like?**	**What does a Near Miss look like? (for avoidance of doubt a near miss should still be reported to IG Team)**
Written Inappropriate Disclosure	Document(s) or correspondence sent to correct recipient but containing data that should not be disclosed (e.g. additional attachments being sent to recipient in addition to the intended attachment and / or information that the recipient did not require). Messages sent to generic email address may be distributed to a whole department / unknown numbers of staff, some of whom may not be appropriate recipients - this could be a breach. Information / data shared with a third party as a result of "blagging" where the third party deceives the employee to obtain data it is not entitled to.	Document(s) recalled or retrieved / double deleted successfully without being read by recipient. Need written evidence of deletion / recall. It may be that following investigation and subject to proof on TMBC systems (e.g. LCS, iCaseWork) data was appropriately shared (including for safeguarding reasons - there is a high threshold for this).
Verbal Inappropriate Disclosure	Data being shared in person or over telephone with incorrect recipient, or sharing data that the recipient did not require. Information / data shared with a third party as a result of "blagging" where the third party deceives the employee to obtain data it is not entitled to.	Very unlikely to be any near miss scenarios. It may be that following investigation and subject to proof on TMBC systems (e.g. LCS, iCaseWork) data was appropriately shared (including for safeguarding reasons - there is a high threshold for this).
Insecure Disposal of Paperwork / physical records	Paperwork not being placed into confidential waste bins for disposal or otherwise disposed of in an unauthorised inappropriate manner.	Paperwork recovered from unsecure disposal and placed correctly in confidential waste bins for shredding
Insecure / incorrect disposal of hardware / removable media	1. Hardware / removable media not returned to IT to dispose of or reformatting for new user. 2. Hardware / removable media passed around service area between users without input or knowledge of IT Team and without necessary measures being taken to remove any data on the hardware. 3. Hardware / removable media disposed of directly by user through unsecure means (putting in own bin / landfill without securing the data first)	Hardware / removable media found immediately and re-directed to IT Team for secure disposable / reformatting as appropriate.

Type of Potential Breach	**What Does a Breach look like?**	**What does a Near Miss look like? <u>(for avoidance of doubt a near miss should still be reported to IG Team)</u>**
System failure	1. Failure of process in a service area leading to inappropriate disclosure of data (e.g. processes not being followed for updating contact details of a service user at first available opportunity, leading to correspondence being incorrectly addressed) 2. Failure of IT system leading to inappropriate disclosure of data (e.g. processes for bulk mailing not formatting correctly leading to incorrect separation of letters. 3. Operator error that has caused or contributed to a third party breach (e.g. error leading to breach by external mail provider such as UKMail or Adare). 4. Writing down password to access system(s) and leaving it on display in an unsecure environment?	Data disclosed through system failure is recovered from recipient without being read, or double deleted without being read. Written proof required.
Inappropriate access to systems	Inappropriate and / or unauthorised access to confidential systems such as LCS / Capita (non-exhaustive list) etc. for personal gain rather than in connection with usual duties of the job role. **This will lead to disciplinary action.**	Very unlikely to be any near miss under this category as any conflicts should be disclosed and access to relevant records blocked. Accidental access to a secure system is likely to fit under system failure rather than this category.
Inaccurate Information Held	1. Inaccurate or out of date information held on TMBC systems (e.g. old address details). 2. Inaccurate data provided to TMBC by third parties which is then held on TMBC systems - this would be a third party breach, but must be reported and logged accordingly. 3. Incomplete processing of data leading to a breach. 4. Rectification request received from individuals (written).	If inaccurate data is rectified upon first discovery and causes no harm or detriment to the data subject, or, if inaccurate information is provided by a third party (IG team should be made aware and notify the third party of their potential breach).

Type of Potential Breach	**What Does a Breach look like?**	**What does a Near Miss look like? (for avoidance of doubt a near miss should still be reported to IG Team)**
Theft of removable media (Disc / external HDD / flash drive	Removable media stolen as a result of poor device security of user. Removable media left unsecured in home, vehicle or in transit making it easier target to steal. Removable media provided by TMBC IT may be encrypted, but media sourced from external parties may not. All removable media should be provided, authorised and secured by IT. Failure to encrypt removable media would be a breach if personal data is held on it.	Unless no personal data was stored on it then very rare for this to be a near miss as even with encryption, likely to be less secure than the user's laptop.
Loss of removable media (Disc / external HDD / flash drive)	As above, but media lost rather than stolen. Media lost in own home or TMBC secure office more likely to be recovered / found, so possibly lower severity than theft of device or loss outside of office / home. All media must be authorised and controlled by IT to ensure safety and encryption. Failure to encrypt removable media would be a breach if personal data is held on it.	Unless no personal data was stored on it, very rare for this to be a near miss, but if after investigation the data on the removable media never existed, or was not stored to the lost removable media at all, therefore no data lost.
Video footage sent to wrong person	Footage sent to incorrect recipient, or additional footage included that the recipient did not require and / or was not authorised to view.	Would only be a near miss if footage does not contain any identifiable data that would allow individual to be identified
Loss of Post by Royal Mail, Courier or other external postal service (likely to be third party breach)	1. Items lost internally at mail service provider. 2. Items lost externally whilst on delivery.	If item lost internally whilst processing by mail provider, it may be recovered by them at a later date and returned to TMBC, or subject to automatic secure destruction. Would depend on the personal data involved.
Email not sent using secure mail	Emailing sensitive data to a third party without appropriate encryption would be considered to be a breach.	
Access to Buildings / IG issues	Inappropriate / unauthorised access to a building that leads to sensitive information being accessed / viewed (e.g. paper files, screens not locked and team whiteboards on display).	All inappropriate access to buildings, including tailgating, needs to be referred to IG Team.

Type of Potential Breach	**What Does a Breach look like?**	**What does a Near Miss look like? (for avoidance of doubt a near miss should still be reported to IG Team)**
Loss of digital data	Personal data breach occurs if data, which allows a living person to be identified, is lost, accidentally or deliberately overwritten or destroyed from shared drives / removable media / casework systems (i.e. LCS, iCaseWork etc.) affecting the availability of that data.	Up to date backup copies of the data kept allowing immediate restoration, or evidence obtained that proves that the data never existed or is not in fact lost. If the data does not fall under definition of personal data, then loss may not constitute a data breach, but may be a conduct issue.
Failure to redact correctly / appropriately	1. Failing to redact data which an individual is not entitled to. 2. Poor quality of redaction and / or incorrect use of redaction software, rendering some or all of data still visible or allowing electronic redaction to be removed / undone. 3. Any hand redaction (marker pen etc.) warrants straight referral to IG as hand redaction should not be used where electronic means are available.	Incorrect / inappropriate redaction caught through internal checks before document(s) is sent to the intended recipient will be near miss, but should be referred to IG Team. Over-redaction is not a breach, but may be a conduct issue.
Failure to use BCC in emails	Any email sent to group of recipients and email addresses included in "To" or "cc" boxes rather than "bcc". Likely only to be generic emails, or data that all parties are entitled to receive or Cc/BCC would not be appropriate at all. Issue is, if not Bcc'd properly, email addresses of all recipients are viewable by all other recipients. Even if double deleted at TMBC request, the personal data (email addresses) will have been visible to all recipients and cannot be fully mitigated. Most likely low risk, but would depend on email details being included - if email addresses included are group / team emails, less likely to be an issue. If individual person's email address, or even their personal email address (as will be the case for many non TMBC recipients) is visible, may be more serious.	Unlikely to be many cases of near miss. Potentially near miss if emails bounce back from all recipients as undeliverable - but that may highlight an incorrect / inaccurate data issue instead.

Type of Potential Breach	**What Does a Breach look like?**	**What does a Near Miss look like? (for avoidance of doubt a near miss should still be reported to IG Team)**
Alteration of Personal Data	Accidental or deliberate alteration of personal data on any TMBC system, or any system held by TMBC's contractual third parties. **Deliberate and / or unauthorised alteration will result in disciplinary action.**	Accidental alteration discovered quickly before it becomes permanent and can be rectified from back up on system. Deliberate and / or unauthorised alteration of records will never be a near miss and will be a disciplinary issue.
Breach of Confidentiality	Disclosing data given to TMBC in confidence without an overriding basis for doing so (e.g. information disclosed is required for legal proceedings and is subject to Order of the Court) or without informing the data subject that confidentiality will be fully or partially waived. If confidential information is to be disclosed, failure to appropriately limit the data disclosed / redact data which should remain confidential may also fall under this category. We would expect a contemporaneous note placing on the CMS and / or file at the time the confidentiality request is made to make clear that confidentiality has been requested from the data subject. If an employee fails to note a confidentiality request on the CMS and or file and another employee subsequently discloses that information, the employee who failed to note the confidentiality request could be implicated in the any data breach.	If confidentiality is waived for a valid reason, clear written evidence needs to be located on the CMS (e.g. LCS, iCaseWork etc.) and / or file relevant to the data being disclosed. Employees must be 100% sure that safeguarding (or any other reason used) is a valid reason to waive confidentiality in any particular case. We would expect a note on the CMS or file setting out the reasons for waiving confidentiality to evidence that consideration has been given. We would also expect that the matter would be discussed with the data subject and recorded in a contemporaneous note on the CMS and or file.
Cyber Security Incident	Brute Force attack, Denial of Service Attack, Malware, Phishing, password cracking, key logging, Ransomware, unauthorised access by third party or other Hardware / Software misconfiguration (including use of unapproved or unlicensed software on Council equipment) leading to inappropriate access to, loss, destruction, alteration or corruption of data.	Incidents caught by and isolated and / or removed by cyber security systems or IT personnel before any data can be affected. Any incident detected by a TMBC employee must be reported immediately to IT with no further action taken until IT direct them - i.e. suspicious emails / attachments not to be opened at all and not to be forwarded to IT unless expressly instructed to do so.

Type of Potential Breach	**What Does a Breach look like?**	**What does a Near Miss look like? <u>(for avoidance of doubt a near miss should still be reported to IG Team)</u>**
Other non-cyber incident	Sweep up category to be used if any new breaches come to light that do not fit the other categories. Possibly breaches arising from environmental factors (fire / flood etc.) may fit in here.	TBC

Appendix 2

Personal Data Breach Reporting Form

Please send the completed form to the Information Governance Team within the first 24 hours of knowledge of the potential breach.

Directorate / Service Area	
Assistant Director	
Service Unit Manager / Line Manager	
Employee Reporting Incident	
Person(s) Responsible for Incident	
Date / Time of Incident	
Date / Time when incident was first reported to management / manager	
Type of Data / Information Involved - (Paper / Email / Letter / Electronic Data)	

	Details of Incident:	
1	Describe in detail what has happened and how the incident has occurred? Outline what data / information is involved? e.g. • Health or Social Care? • Financial (e.g. Bank details)? • Personally Identifiable Information (e.g. Name, Address, NI Number)? • Sensitive information (e.g. Religion, gender, sex or medical details)?	
2	Did the employee self-report the incident?	☐ Yes ☐ No
3	Has the individual responsible for the incident undertaken the mandatory data protection training? If so when?	☐ Yes ☐ No Training completed on:
4	Are there any mitigating circumstances put forward by the employee as to why it happened?	
	Documents / Emails Only	
5	If relating to a document / email has it been opened / read by the wrong recipient?	☐ Yes ☐ No

	Please attach a copy of any letter / document(s) inadvertently disclosed.	
6	**If No**, and the document / email has not been opened / read, has the document / email been double deleted (email), destroyed and / or recovered?	☐ Double deleted (from mailbox and deleted folder) ☐ Destroyed ☐ Recovered (must be recovered unopened / unread) If you have ticked one of the above boxes **and** can provide evidence of the destruction / recovery, proceed to question 16
	Electronic Devices Only	
7	If reporting that a mobile device has been lost or stolen, has it been reported to ICT? Please provide the name of the contact and date?	☐ Yes ☐ No
8	Was it encrypted or password protected?	☐ Yes ☐ No
9	Was the password / code stored with the device?	☐ Yes ☐ No
10	Were any paper records containing personal data stored with the device? Please describe what paper records were stored with the device.	☐ Yes ☐ No
	General Questions	
11	Number of personal data records concerned?	
12	How many data subjects could be affected?	
13	What is the likelihood that data subjects will experience significant consequences because of the incident? (Impact on health, wellbeing, family life, finances, community relationships etc.)	☐ Very Likely ☐ Likely ☐ Neutral – neither likely nor unlikely ☐ Unlikely ☐ Very Unlikely ☐ Unknown

14	Please set out your reasoning for your answer to question 13 above	
15	Does the incident present any immediate safeguarding concerns? Please outline the safeguarding concerns:	☐ Yes ☐ No
16	Please categorise the reason for the incident?	☐ Lack of attention / Human Error ☐ Systems / Process failure ☐ Lack of training ☐ Checker failed to spot error
17	Is the incident a one off or has more than one incident occurred? Please provide details of previous incidents?	
18	Please can you detail what learning can be established and implemented from the incident to prevent similar incidents from occurring in the future?	
19	Has there been any media coverage of the incident? **If yes**, please advise what media coverage has taken place. If possible provide links to the coverage or attach a copy with this form.	☐ Yes ☐ No
20	Are any other partners involved? (Do we need to tell any other organisations about the breach)?	
	Immediate Action Taken:	
21	Have you taken any action to reduce the effect on the data subjects involved? If so please provide details:	☐ Yes ☐ No
22	Have you told the data subjects about the breach?	☐ Yes ☐ No

		NB if you have not yet notified the data subject, please do not do so without agreement from the Information Governance Team.

To be completed by the Manager submitting the Incident Form

Name: Signature: Date: Job Title:

Return to the Risk, Insurance and Information Governance Team by emailing information.governance@tameside.gov.uk copying in your Assistant Director