MINUTES OF A MEETING OF
THE POLICY AND RESOURCES COMMITTEE
MALVERN TOWN COUNCIL
held in the Council Chamber, Belle Vue Terrace, Malvern
on Monday 13 May 2024 at 6.00 pm

Councillors
I Dawson (Chair)
N Houghton
M Jones
L Lowton (substitute for Cllr M Birks)
D Mead (substitute for Cllr C Fletcher)
R McLaverty-Head
J MacLusky
K Newbigging

Absent
M Birks (apologies)
C Fletcher (apologies)

Also in attendance
Linda Blake - Town Clerk
Louise Wall – Minute Clerk

Cllr David Watkins

1. APOLOGIES FOR ABSENCE

Apologies for absence from Cllr Marilyn Birks and Cllr Clive Fletcher were **NOTED.** Cllr Birks had substituted Cllr Lou Lowton and Cllr Fletcher had substituted Cllr David Mead.

2. DECLARATIONS OF INTEREST

None.

3. MINUTES OF PREVIOUS MEETING

It was **RESOLVED** that the minutes of the following meeting be approved and adopted as a correct record of the proceedings, to be signed by the Chairman:

- Policy and Resources Committee meeting held on 27 March 2024.

PUBLIC PARTICIPATION

None.

4. SMALL GRANTS SCHEME, 2ND ROUND 2023/24 – EDEN ESOL

Report PR01/24 was received and accepted.

The Town Clerk had received written confirmation from Eden ESOL that English teaching is separate from the activities of the church.

It was **AGREED** to award a grant of £467.90 to Eden ESOL.

5. PHOTOCOPIER CONTRACT

Report PR02/24 was received and accepted.

The Town Clerk explained that the photocopier lease was now due for renewal and had sought quotations from several companies, which were tabled in the report.

It was **AGREED** to award a five-year photocopier lease contract to Company C (Dolphintec).

6. FINANCIAL REPORTS

The financial reports were received and accepted, along with the cash report CR1 and the bank payments schedules for January, February and March 2024.

The Town Clerk explained some of the main points of the report:

- The bank schedules showed some large payments relating to the new building, which meant the bank balance was lower than usual as a result of these.
- Creditor days outstanding – the target is 30 days, although officers aim to pay smaller local companies as soon as possible. Creditor days were 23.41 at the end of January, and 27/49 at the end of February but had fallen to 0.61 at the end of March due to a large payment for the community hub building which needed to be settled within the month.
- Bad debts – there had been two bad debtors in the period, one was a football team that had struggled to pay high electricity bills and the other was the lengthsman scheme which was paid late due to a billing enquiry. Both had now been cleared.
- All payments went through a process of being checked by two councillors, one officer and the Town Clerk, which was a robust process and good practice.

Committee **NOTED** the financial reports for January, February, and March 2024.

7. CCTV POLICY

Report PR04/24 was received and accepted.

The Town Clerk explained that the requirements for small organisations operating CCTV equipment, as set out by the Information Commissioner's office, were adhered to already by the Town Council, except for the need to have a CCTV policy in place. Members were asked to review and comment on the draft policy in the report.

Members discussed the policy and raised the following points:

- It was important to make clear to employees that they would not be monitored in their day-to-day work.
  - Clarification will be added that the cameras are to monitor the exterior of the building only.
- The CCTV policy should be connected to the Data Protection policy.
  - A cross reference will be inserted into the CCTV policy.
- Cameras should not record or overlook private property.
  - Cameras have been installed to monitor the exterior of the building only, but if they should cover any parts of private property, this can be obscured by the CCTV company.
- As the policy would be a new one, it should be reviewed in twelve months' time.

It was **RECOMMENDED** that a closed-circuit television (CCTV) policy is adopted by the Town Council. A draft of the policy is attached to these minutes.

8. REVIEW OF DATA PROTECTION POLICY

Report PR05/24 was received and accepted.

The last review of the Data Protection Policy had taken place in December 2019. Members were asked to consider the current policy as well as a template supplied by the National Association of Local Councils (NALC), and recommend any amendments.

It was **RECOMMENDED** that the Town Council adopts NALC's Data Protection Policy for Staff. A draft of the policy is attached to these minutes.

9. DATE AND TIME OF NEXT MEETING

It was **AGREED** that the date of the next meeting would be Wednesday 12 June 2024 at 6pm.

The meeting finished at 6.20pm

……(Chairman)

MALVERN TOWN COUNCIL

DRAFT DATA PROTECTION POLICY FOR COUNCIL EMPLOYEES

Reviewed by:	Policy and Resources Committee – 13 May 2024
Adopted:	Full Council – 15 May 2024
Next review due:	May 2028

MALVERN TOWN COUNCIL

DATA PROTECTION POLICY

1. Purpose

1.1. Malvern Town Council (hereafter known as 'the Council') is committed to being transparent about how it collects and uses the personal data of staff, and to meeting its data protection obligations. This policy sets out the Council's commitment to data protection, and your rights and obligations in relation to personal data in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

1.2. This policy applies to the personal data of current and former job applicants, employees, workers, contractors, and former employees, referred to as HR-related personal data. This policy does not apply to the personal data relating to members of the public or other personal data processed for council business.

1.3. The Council has appointed Linda Blake, Town Clerk, as the person with responsibility for data protection compliance within the council. Questions about this policy, or requests for further information, should be directed to them.

2. Definitions

2.1. "Personal data" is any information that relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information. It includes both automated personal data and manual filing systems where personal data are accessible according to specific criteria. It does not include anonymised data.

2.2. "Processing" is any use that is made of data, including collecting, recording, organising, consulting, storing, amending, disclosing or destroying it.

2.3. "Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data as well as criminal convictions and offences.

2.4. "Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3. Data protection principles

3.1. The Council processes HR-related personal data in accordance with the following data protection principles the council:

- processes personal data lawfully, fairly and in a transparent manner
- collects personal data only for specified, explicit and legitimate purposes
- processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- keeps personal data only for the period necessary for processing
- adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage

3.2. The Council will tell you of the personal data it processes, the reasons for processing your personal data, how it uses such data, how long it retains the data, and the legal basis for processing in its privacy notices.

3.3. The Council will not use your personal data for an unrelated purpose without telling you about it and the legal basis that it intends to rely on for processing it. The Council will not process your personal data if it does not have a legal basis for processing.

3.4. The Council keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

4. Processing

Personal data

4.1. The Council will process your personal data (that is not classed as special categories of personal data) for one or more of the following reasons:

- it is necessary for the performance of a contract, e.g., your contract of employment (or services); and/or
- it is necessary to comply with any legal obligation; and/or
- it is necessary for the council's legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect your personal data which overrides those legitimate interests; and/or
- it is necessary to protect the vital interests of a data subject or another person; and/or
- it is necessary for the performance if a task carried out in the public interest or in the exercise of official authority vested in the controller.

4.2. If the Council processes your personal data (excluding special categories of personal data) in line with one of the above bases, it does not require your consent. Otherwise, the Council

is required to gain your consent to process your personal data. If the Council asks for your consent to process personal data, then it will explain the reason for the request. You do not need to consent or can withdraw consent later.

4.3. The Council will not use your personal data for an unrelated purpose without telling you about it and the legal basis that it intends to rely on for processing it.

4.4. Personal data gathered during the employment is held in your personnel file in hard copy and electronic format on HR and IT systems and servers. The periods for which the Council holds your HR-related personal data are contained in its privacy notices to individuals.

4.5. Sometimes the Council will share your personal data with contractors and agents to carry out its obligations under a contract with the individual or for its legitimate interests. The Council requires those individuals or companies to keep your personal data confidential and secure and to protect it in accordance with Data Protection law and the Council's policies. They are only permitted to process that data for the lawful purpose for which it has been shared and in accordance with the Council's instructions.

4.6. The Council will update HR-related personal data promptly if you advise that your information has changed or is inaccurate. You may be required to provide documentary evidence in some circumstances.

4.7. The Council keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Special categories of data

4.8. The Council will only process special categories of your personal data (see above) on the following basis in accordance with legislation:

- where it is necessary for carrying out rights and obligations under employment law or a collective agreement;
- where it is necessary to protect your vital interests or those of another person where you are physically or legally incapable of giving consent;
- where you have made the data public;
- where it is necessary for the establishment, exercise or defence of legal claims;
- where it is necessary for the purposes of occupational medicine or for the assessment of your working capacity;
- where it is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates to only members or former members provided there is no disclosure to a third party without consent;

- where it is necessary for reasons for substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards;
- where is it necessary for reasons of public interest in the area of public health; and
- where is it necessary for archiving purposes in the public interest or scientific and historical research purposes.

4.9. If the Council processes special categories of your personal data in line with one of the above bases, it does not require your consent. In other cases, the Council is required to gain your consent to process your special categories of personal data. If the Council asks for your consent to process a special category of personal data, then it will explain the reason for the request. You do not have to consent or can withdraw consent later.

5. Individual rights

5.1. As a data subject, you have a number of rights in relation to your personal data.

Subject access requests

5.2. You have the right to make a subject access request. If you make a subject access request, the Council will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from yourself;
- to whom your data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long your personal data is stored (or how that period is decided);
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think the council has failed to comply with your data protection rights; and
- whether or not the council carries out automated decision-making and the logic involved in any such decision-making.

5.3. The Council will also provide you with a copy of your personal data undergoing processing. This will normally be in electronic form if you have made a request electronically, unless you agree otherwise.

5.4. If you want additional copies, the Council may charge a fee, which will be based on the administrative cost to the council of providing the additional copies.

5.5. To make a subject access request, you should send the request to the Town Clerk. In some cases, the Council may need to ask for proof of identification before the request can be

processed. The Council will inform you if we need to verify your identity and the documents it requires.

5.6. The Council will normally respond to a request within a period of one month from the date it is received. Where the Council processes large amounts of your data, this may not be possible within one month. The Council will write to you within one month of receiving the original request to tell you if this is the case.

5.7. If a subject access request is manifestly unfounded or excessive, the Council is not obliged to comply with it. Alternatively, the Council can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Council has already responded. If you submit a request that is unfounded or excessive, the Council will notify you that this is the case and whether or not it will respond to it.

Other rights

5.8. You have a number of other rights in relation to your personal data. You can require the council to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override the Council's legitimate grounds for processing data (where the Council relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override the Council's legitimate grounds for processing data.
- complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk).

5.9. To ask the Council to take any of these steps, you should send the request to the Town Clerk.

6. Data security

6.1. The Council takes the security of HR-related personal data seriously. The Council has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

6.2. Where the Council engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments

6.3. Some of the processing that the Council carries out may result in risks to privacy (such as monitoring of public areas via CCTV). Where processing would result in a high risk to your rights and freedoms, the Council will carry out a data protection impact assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for yourself and the measures that can be put in place to mitigate those risks.

Data breaches

6.4. The Council have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur the Council must take notes and keep evidence of that breach.

6.5. If you are aware of a data breach you must contact the Town Clerk immediately and keep any evidence you have in relation to the breach.

6.6. If the Council discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of yourself, the Council will report it to the Information Commissioner within 72 hours of discovery. The Council will record all data breaches regardless of their effect.

6.7. If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Council will tell you that there has been a breach and provide you with information about its likely consequences and the mitigation measures it has taken.

International data transfers

6.8. The Council will not transfer HR-related personal data to countries outside the EEA.

Individual responsibilities

6.9. You are responsible for helping the Council keep your personal data up to date. You should let the Council know if data provided to the Council changes, for example if you move to a new house or change your bank details.

6.10. Everyone who works for, or on behalf of, the Council has some responsibility for ensuring data is collected, stored and handled appropriately, in line with the Council's policies.

6.11. You may have access to the personal data of other individuals and of members of the public in the course of your work with the Council. Where this is the case, the Council relies on you to help meet its data protection obligations to employees and members of the public. Individuals who have access to personal data are required:

- to access only data that you have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Council) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, locking computer screens when away from desk, and secure file storage and destruction including locking drawers and cabinets, not leaving documents on desk whilst unattended);
- not to remove personal data, or devices containing or that can be used to access personal data, from the council's premises without prior authorisation and without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.
- to never transfer personal data outside the European Economic Area except in compliance with the law and with express authorisation from the Town Clerk or Chair of the Council
- to ask for help from the Council's data protection lead if unsure about data protection or if you notice a potential breach or any areas of data protection or security that can be improved upon.

6.12. Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Council's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so or concealing or destroying personal data as part of a subject access request, may constitute gross misconduct and could lead to dismissal without notice.

MALVERN TOWN COUNCIL

DRAFT DATA PROTECTION POLICY FOR COUNCIL EMPLOYEES

Reviewed by:	Policy and Resources Committee – 13 May 2024
Adopted:	Full Council – 15 May 2024
Next review due:	May 2028

MALVERN TOWN COUNCIL

DATA PROTECTION POLICY

1. Purpose

1.1. Malvern Town Council (hereafter known as 'the Council') is committed to being transparent about how it collects and uses the personal data of staff, and to meeting its data protection obligations. This policy sets out the Council's commitment to data protection, and your rights and obligations in relation to personal data in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

1.2. This policy applies to the personal data of current and former job applicants, employees, workers, contractors, and former employees, referred to as HR-related personal data. This policy does not apply to the personal data relating to members of the public or other personal data processed for council business.

1.3. The Council has appointed Linda Blake, Town Clerk, as the person with responsibility for data protection compliance within the council. Questions about this policy, or requests for further information, should be directed to them.

2. Definitions

2.1. "Personal data" is any information that relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information. It includes both automated personal data and manual filing systems where personal data are accessible according to specific criteria. It does not include anonymised data.

2.2. "Processing" is any use that is made of data, including collecting, recording, organising, consulting, storing, amending, disclosing or destroying it.

2.3. "Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data as well as criminal convictions and offences.

2.4. "Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3. Data protection principles

3.1. The Council processes HR-related personal data in accordance with the following data protection principles the council:

- processes personal data lawfully, fairly and in a transparent manner
- collects personal data only for specified, explicit and legitimate purposes
- processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- keeps personal data only for the period necessary for processing
- adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage

3.2. The Council will tell you of the personal data it processes, the reasons for processing your personal data, how it uses such data, how long it retains the data, and the legal basis for processing in its privacy notices.

3.3. The Council will not use your personal data for an unrelated purpose without telling you about it and the legal basis that it intends to rely on for processing it. The Council will not process your personal data if it does not have a legal basis for processing.

3.4. The Council keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

4. Processing

Personal data

4.1. The Council will process your personal data (that is not classed as special categories of personal data) for one or more of the following reasons:

- it is necessary for the performance of a contract, e.g., your contract of employment (or services); and/or
- it is necessary to comply with any legal obligation; and/or
- it is necessary for the council's legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect your personal data which overrides those legitimate interests; and/or
- it is necessary to protect the vital interests of a data subject or another person; and/or
- it is necessary for the performance if a task carried out in the public interest or in the exercise of official authority vested in the controller.

4.2. If the Council processes your personal data (excluding special categories of personal data) in line with one of the above bases, it does not require your consent. Otherwise, the Council

is required to gain your consent to process your personal data. If the Council asks for your consent to process personal data, then it will explain the reason for the request. You do not need to consent or can withdraw consent later.

4.3. The Council will not use your personal data for an unrelated purpose without telling you about it and the legal basis that it intends to rely on for processing it.

4.4. Personal data gathered during the employment is held in your personnel file in hard copy and electronic format on HR and IT systems and servers. The periods for which the Council holds your HR-related personal data are contained in its privacy notices to individuals.

4.5. Sometimes the Council will share your personal data with contractors and agents to carry out its obligations under a contract with the individual or for its legitimate interests. The Council requires those individuals or companies to keep your personal data confidential and secure and to protect it in accordance with Data Protection law and the Council's policies. They are only permitted to process that data for the lawful purpose for which it has been shared and in accordance with the Council's instructions.

4.6. The Council will update HR-related personal data promptly if you advise that your information has changed or is inaccurate. You may be required to provide documentary evidence in some circumstances.

4.7. The Council keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Special categories of data

4.8. The Council will only process special categories of your personal data (see above) on the following basis in accordance with legislation:

- where it is necessary for carrying out rights and obligations under employment law or a collective agreement;
- where it is necessary to protect your vital interests or those of another person where you are physically or legally incapable of giving consent;
- where you have made the data public;
- where it is necessary for the establishment, exercise or defence of legal claims;
- where it is necessary for the purposes of occupational medicine or for the assessment of your working capacity;
- where it is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates to only members or former members provided there is no disclosure to a third party without consent;

- where it is necessary for reasons for substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards;
- where is it necessary for reasons of public interest in the area of public health; and
- where is it necessary for archiving purposes in the public interest or scientific and historical research purposes.

4.9. If the Council processes special categories of your personal data in line with one of the above bases, it does not require your consent. In other cases, the Council is required to gain your consent to process your special categories of personal data. If the Council asks for your consent to process a special category of personal data, then it will explain the reason for the request. You do not have to consent or can withdraw consent later.

5. Individual rights

5.1. As a data subject, you have a number of rights in relation to your personal data.

Subject access requests

5.2. You have the right to make a subject access request. If you make a subject access request, the Council will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from yourself;
- to whom your data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long your personal data is stored (or how that period is decided);
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think the council has failed to comply with your data protection rights; and
- whether or not the council carries out automated decision-making and the logic involved in any such decision-making.

5.3. The Council will also provide you with a copy of your personal data undergoing processing. This will normally be in electronic form if you have made a request electronically, unless you agree otherwise.

5.4. If you want additional copies, the Council may charge a fee, which will be based on the administrative cost to the council of providing the additional copies.

5.5. To make a subject access request, you should send the request to the Town Clerk. In some cases, the Council may need to ask for proof of identification before the request can be

processed. The Council will inform you if we need to verify your identity and the documents it requires.

5.6. The Council will normally respond to a request within a period of one month from the date it is received. Where the Council processes large amounts of your data, this may not be possible within one month. The Council will write to you within one month of receiving the original request to tell you if this is the case.

5.7. If a subject access request is manifestly unfounded or excessive, the Council is not obliged to comply with it. Alternatively, the Council can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Council has already responded. If you submit a request that is unfounded or excessive, the Council will notify you that this is the case and whether or not it will respond to it.

Other rights

5.8. You have a number of other rights in relation to your personal data. You can require the council to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override the Council's legitimate grounds for processing data (where the Council relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override the Council's legitimate grounds for processing data.
- complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk).

5.9. To ask the Council to take any of these steps, you should send the request to the Town Clerk.

6. Data security

6.1. The Council takes the security of HR-related personal data seriously. The Council has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

6.2. Where the Council engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments

6.3. Some of the processing that the Council carries out may result in risks to privacy (such as monitoring of public areas via CCTV). Where processing would result in a high risk to your rights and freedoms, the Council will carry out a data protection impact assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for yourself and the measures that can be put in place to mitigate those risks.

Data breaches

6.4. The Council have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur the Council must take notes and keep evidence of that breach.

6.5. If you are aware of a data breach you must contact the Town Clerk immediately and keep any evidence you have in relation to the breach.

6.6. If the Council discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of yourself, the Council will report it to the Information Commissioner within 72 hours of discovery. The Council will record all data breaches regardless of their effect.

6.7. If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Council will tell you that there has been a breach and provide you with information about its likely consequences and the mitigation measures it has taken.

International data transfers

6.8. The Council will not transfer HR-related personal data to countries outside the EEA.

Individual responsibilities

6.9. You are responsible for helping the Council keep your personal data up to date. You should let the Council know if data provided to the Council changes, for example if you move to a new house or change your bank details.

6.10. Everyone who works for, or on behalf of, the Council has some responsibility for ensuring data is collected, stored and handled appropriately, in line with the Council's policies.

6.11. You may have access to the personal data of other individuals and of members of the public in the course of your work with the Council. Where this is the case, the Council relies on you to help meet its data protection obligations to employees and members of the public. Individuals who have access to personal data are required:

- to access only data that you have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Council) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, locking computer screens when away from desk, and secure file storage and destruction including locking drawers and cabinets, not leaving documents on desk whilst unattended);
- not to remove personal data, or devices containing or that can be used to access personal data, from the council's premises without prior authorisation and without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.
- to never transfer personal data outside the European Economic Area except in compliance with the law and with express authorisation from the Town Clerk or Chair of the Council
- to ask for help from the Council's data protection lead if unsure about data protection or if you notice a potential breach or any areas of data protection or security that can be improved upon.

6.12. Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Council's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so or concealing or destroying personal data as part of a subject access request, may constitute gross misconduct and could lead to dismissal without notice.