Elloughton cum Brough Town Council
60 Welton Road, Brough, HU15 1BH
Write to: PO Box 124, Brough, HU15 1YH
Telephone: 01482 665600
Website: elloughtonbrough-tc.gov.uk

GDPR Policy Pack

Policy pack includes:

- Bring Your Own Device Policy
- Data Protection Policy
- General Privacy Notice (GDPR)
- Privacy Notice for Staff*, Councillors and Role Holders**(GDPR)
- Privacy Policy.(GDPR)
- Subject Access Request Policy (GDPR)
- Data Consent Form

Document History

Adopted by COUNCIL – 15th May 2023
To be reviewed – May 2024

Philippa Beverley
Town Clerk

Elloughton cum Brough Town Council
60 Welton Road, Brough, HU15 1BH
Write to: PO Box 124, Brough, HU15 1YH
Telephone: 01482 665600
Website: elloughtonbrough-tc.gov.uk

Bring Your Own Device Policy

Philippa Beverley
Town Clerk

1. INTRODUCTION

1.1 The use of personal mobile devices, such as smartphones, laptops and tablets in connection with Town Council's business is a privilege granted to specific employees through approval of their management.

1.2 The Council reserves the right to revoke these privileges if Users do not abide by the policies and procedures set out in its 'Bring Your Own Device Policy' (BYOD) Policy.

1.3 These policies are in place to protect the integrity and effective operation of the Council's data, information and communications systems to ensure they remain safe, secure and available for carrying out the Council's business, including:

- To protect devices and systems from downtime, caused by malware and viruses.
- To protect systems and information that is necessary to business processes, which would present risk to the operational requirements of the business.
- To protect information where access must be restricted to certain groups or individuals.
- To protect the value of the information to the company e.g. intellectual property, commercially sensitive information.
- To protect confidential information because of legal obligations, such as personal data under the Data Protection Act or payment card PCI-DSS regulations.
- To protect information included in regulatory requirements, such as financial data.
- To protect information that is externally owned or provided, such as those defined in contracts.
- To protect information that is important to health and safety.

1.4 This policy document covers the many areas, in a simple and concise format, which are necessary to manage and secure our BYOD environment while enabling you to be more productive.

2. USER ELIGIBILITY

2.1 The Council's BYOD policy applies to all employees that use personal devices and to consultants and other temporary workers, who require access to specific systems to carry out their duties.

2.2 The Council may limit what data or systems that can be accessed by personal owned devices.

2.3 Users with personally owned devices can access the following list of applications according to their role within the company, and the type of personal device: **Office 365**.

2.4 The User must understand the consequences of installing personal applications on personal devices used to access the Council's networks, information and communications systems. These can introduce malware into systems, or result in exposing confidential data held, to theft or loss.

2.5 Best practise includes:
- Use only well-known and well-respected application vendors.
- Use any Council App repositories intended for personal devices. From time to time the Council may sign up to popular Mobile apps used by employees.
- Maintain up-to-date security software on personal device(s).
- Automatically run/accept regular updates of the application software Privacy the Council is committed to protecting the privacy of Users enrolled in its BYOD programme.

2.6 The Council will permanently delete all its records of an inadvertent contact with a User's personal data and inform the User as soon as discovered and practical.

2.7 The Council will never search a User's device data without the prior consent of the User.

2.8 If the User device has been contaminated with malware, which presents a risk to the Council's data and its systems, then it has the right to wipe the whole device, which may result in the loss of personal and business data. The Council will make every effort to communicate with the User BEFORE these actions are taken.

2.9 The Council disclaims any liability for loss of personal applications or data, whether directly or indirectly resulting from the usage of company information and communications systems, and/or the wiping of company apps or data, or the removal of malware or the wiping of the whole device.

2.10 The Council does not accept any financial responsibility for mobile phone, mobile data and public WIFI services incurred by the User.

2.11 The User is responsible for reporting lost or stolen devices or breaches of security on personal owned devices to the IT Service Desk in the first instance.

2.12 Upon leaving employment the **User MUST** remove all Council information, applications, passwords, data and APPs from personally owned devices upon separation from the Council or at the Council's request.

2.13 The Council may/will require checking and/or wiping of any company data held on personal devices.

2.14 Any Council owned, licensed and installed software on personally owned devices is required to be reconciled. Depending on the type of license:
- The Council may request the User to reimburse the Council for the software, or
- The Council may request the User destroy the software, or
- The Council may decide to allow the User to keep software with no further value.

2.15 The Council will only support company applications, network and User access/login to the Council's systems, and company software/configuration installed on personal devices.

2.16 The Council will not support any mobile applications for personal use and consumption.

2.17 The Council will not provide support for broken personal devices.

2.18 The Council reserves the right to revoke the privileges to use personal devices if Users do not abide by the Council's policies and procedures.

2.19 If the User circumvents configurations, security, access and practices then the User will be in violation of the Council's BYOD Policy.

2.20 Policy violations will/may be subject to warnings or disciplinary action as per the Council's Terms and Conditions of Employment.

3. DEVICE REGISTRATION AND COMPLIANCE

3.1 The Council reserves the right to have Users register and receive consent to connect to the Council's network, information and communications systems.

4. USER AGREEMENT AND RESPONSIBILITIES

4.1 **The User MUST** comply with the Council's BYOD policy terms and conditions.

4.2 **The User MUST** contribute to the protection of the Council's data, applications, information and communications systems by exercising caution, being aware of the risks, complying with the Council's security requirements and security best practices.

4.3 The Council retains ownership of all the business data, documents and files, intellectual property and secure-access information and has the right and obligation to govern this data.

4.4 The User agrees that the Council may require them to implement specific device configurations or software before the User is allowed access to Council data, applications, networks, information and communications systems. If the User disagrees with any of these requirements, they will not be allowed access from their own device(s), or may only gain access to certain systems, or may only be given guest access to the Internet.

4.5 The Council and the User must comply with all regulations and laws. These laws and regulations might require the Council to access its data on your personal device(s), or you may be compelled to provide or remove any such data from your personal device(s).

5. ACCEPTABLE USE

5.1 **The User MUST** follow all administrative and acceptable use policies when a personal owned device is connected to the Council's networks, information and communications systems or where social media and/or collaboration solutions are applied for business purposes.

5.2 **The User MUST** ensure that when they use their personal device for personal reasons, that they are not using the Council's intellectual property

rights, any business confidential data, or any data that may be regulated or protected under European or UK legislation.

5.3 The Council retains the right to perform operations on a personally owned device, such as scanning for malware, or checking security configurations. The User will be made aware of how and when these operations will be carried out.

5.4 **The User MUST** consider the sensitivity of the Council's data held on the personal owned device, when sharing the device with family and friends.

5.5 **The User MUST** report **IMMEDIATELY** any data breaches, disclosures or malware infections on personally owned devices to the Council immediately they become aware.

5.6 As a condition of access to company data and ICT resources, the User is required to install security software and activate the devices firewall.

5.7 The User MUST regularly update and/or accept updates to OS software directly provided by the devices manufacturer or service provider.

5.8 If the User device has been contaminated with malware, which presents a risk to the Council's data and its systems, then it has the right to wipe the whole device, which may result in the loss of personal and business data. The Council will make every effort to communicate with the User **BEFORE** these actions are taken.

5.9 Jailbreaking, rooting and modifications to the personal device OS are **PROHIBITED**.

5.10 **The User MUST** back-up or synchronise any company data/information held on their personal device with company systems.

5.11 **The User MUST** ensure that any device that is to be replaced or thrown away must have the permanent memory wiped.

6. LOGINS, PASSWORDS, PINS AND AUTHENTICATION

6.1 The Council will issue Logins and Passwords for access to its network, applications, information and communications systems - as it does with company-owned devices. This information MUST never be passed on to third parties or communicated on personal social networks.

6.2 The User **MUST** ensure there is a PIN or Login to operate any personal owned devices before access to the Council's networks, information systems, applications and data can be granted.

6.3 The Council may require device PINs and passwords to be changed regularly, to comply with its security policies, regulatory or legal requirements.

6.4 The Council may enforce the use of passwords for personal owned devices to comply with its policy or any data governance.

6.5 The Council may block access for devices with out-of-date passwords, or passwords with a low strength.

6.6 Where the Council uses additional security techniques to secure its data and systems, such as two-factor authentication, the User **MUST** use such systems with their personal device where directed.

6.7 The User has a responsibility towards the safeguarding of company and confidential data in their possession. It is best practice to encrypt confidential data on mobile devices in case of loss or theft.

6.8 Where the Council must comply with industry regulations and legislation, the User MUST encrypt all confidential data held on mobile personal device(s). In these circumstances the company has the right to monitor, check and prevent access for any devices without encryption.

6.9 The User should allow any of the Council's appointed 3rd party organisation to access personal device for audit and checking purposes.

6.10 The Council may deploy software on personal devices of an enrolled User so that they adhere to the Council's platform and operating system (OS) version policy or security policies.

6.11 The Council will inform the User about any device management and policy enforcement processes that it does/will apply.

6.12 If a User does not want their personal device to be managed or have policies enforced, then they may/will not be allowed access to the Council's network, information and communications systems, or the User may be given limited access to company systems.

Elloughton cum Brough Town Council
60 Welton Road, Brough, HU15 1BH
Write to: PO Box 124, Brough, HU15 1YH
Telephone: 01482 665600
Website: elloughtonbrough-tc.gov.uk

Data Protection Policy

Philippa Beverley
Town Clerk

1. Introduction

1.5 The Town Council recognises its responsibility to comply with the General Data Protection Regulations (GDPR) 2018 which regulates the use of personal data. This does not have to be sensitive data; it can be as little as a name and address.

2. General Data Protection Regulations (GDPR)

2.1 The GDPR sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used.

2.2 The GDPR applies to anyone holding personal information about people, electronically or on paper. The Town Council has also notified the Information Commissioner that it holds personal data about individuals.

2.3 When dealing with personal data, Town Council staff and members must ensure that:

- Data is processed fairly, lawfully and in a transparent manner this means that personal information should only be collected from individuals if staff have been open and honest about why they want the personal information.
- Data is processed for specified purposes only this means that data is collected for specific, explicit and legitimate purposes only.
- Data is relevant to what it is needed for.
- Data will be monitored so that too much or too little is not kept; only data that is needed should be held.
- Data is accurate and kept up to date and is not kept longer than it is needed.
- Personal data should be accurate, if it is not, it should be corrected. Data no longer needed will be shredded or securely disposed of.
- Data is processed in accordance with the rights of individuals.
- Individuals must be informed, upon request, of all the personal information held about them.
- Data is kept securely.
- There should be protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

3. Storing and accessing data

3.2 The Town Council recognises its responsibility to be open with people when taking personal details from them. This means that staff must be honest about why they want a particular piece of personal information.

3.3 The Town Council may hold personal information about individuals such as their names, addresses, email addresses and telephone numbers. These will

be securely kept at the Town Council Office and are not available for public access.

3.4 All data stored on the Town Council Office computers are password protected. Once data is not needed any more, is out of date or has served its use and falls outside the minimum retention time of Councils document retention policy, it will be shredded or securely deleted from the computer.

3.5 The Town Council is aware that people have the right to access any personal information that is held about them. Subject Access Requests (SARs) must be submitted in writing (this can be done in hard copy, email or social media). If a person requests to see any data that is being held about them, the SAR response must detail:

- How and to what purpose personal data is processed.
- Anyone who has access to the personal data.

3.6 The response must be sent within 30 days and should be free of charge.

3.7 If a SAR includes personal data of other individuals, the Town Council must not disclose the personal information of the other individual. That individual's personal information may either be redacted, or the individual may be contacted to give permission for their information to be shared with the Subject.

3.8 Individuals have the right to have their data rectified if it is incorrect, the right to request erasure of the data, the right to request restriction of processing of the data and the right to object to data processing, although rules do apply to those requests.

3.9 Please see "Subject Access Request Procedure" for more details.

4. Confidentiality

4.6 The Town Council members and staff must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential

Elloughton cum Brough Town Council
60 Welton Road, Brough, HU15 1BH
Write to: PO Box 124, Brough, HU15 1YH
Telephone: 01482 665600
Website: elloughtonbrough-tc.gov.uk

General Privacy Notice (GDPR)

Philippa Beverley
Town Clerk

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by the **Elloughton cum Brough Town Council** which is the data controller for your data.

Other data controllers the council works with:

- Elloughton cum Brough Town Council and the East Riding of Yorkshire Council
- Community groups
- Charities
- Other not for profit entities
- Contractors

We may need to share your personal data we hold with them so that they can carry out their responsibilities to the council. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the council and the other data controllers may be "joint data controllers" which mean we are all collectively responsible to you for your data. Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant data controller.

A description of what personal data the council processes and for what purposes is set out in this Privacy Notice.

The council will process some or all of the following personal data where necessary to perform its tasks:

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by a council, or where you provide them to us, we may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you pay for activities such as use of a council hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;

- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation.

How we use sensitive personal data

- We may process sensitive personal data including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

We use your personal data for some or all of the following purposes:

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
- To confirm your identity to provide some services;
- To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);
- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our facilities, services, events and staff, councillors and other role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council, and;
- To allow the statistical analysis of data so we can plan the provision of services.

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

What is the legal basis for processing your personal data?

The council is a public authority and has certain powers and obligations. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the council's statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services. We will always take into account your interests and rights. This Privacy Notice sets out your rights and the council's obligations to you.

We may process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy

Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

Sharing your personal data

This section provides information about the third parties with whom the council may share your personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- The data controllers listed above under the heading "Other data controllers the council works with";
- Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data:

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1) The right to access personal data we hold on you

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2) ***The right to correct and update the personal data we hold on you***

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3) ***The right to have your personal data erased***

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
- When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4) ***The right to object to processing of your personal data or to restrict it to certain purposes only***

- You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5) ***The right to data portability***

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6) ***The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained***

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7) ***The right to lodge a complaint with the Information Commissioner's Office.***

- You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on our website **elloughtonbrough-tc.gov.uk**

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints to **The Data Controller, Philippa Beverley,** in the following ways:

Address: **Elloughton cum Brough, 60 Welton Road, Brough, HU15 1BH**
Telephone: **01482 665600**
Email: **elloughtonbrough-tc.gov.uk**

Elloughton cum Brough Town Council
60 Welton Road, Brough, HU15 1BH
Write to: PO Box 124, Brough, HU15 1YH
Telephone: 01482 665600
Website: elloughtonbrough-tc.gov.uk

Privacy Notice for Staff*, Councillors and Role Holders** (GDPR)

Philippa Beverley
Town Clerk

*"Staff" means employees, workers, agency staff and those retained on a temporary or permanent basis.

** "Role Holders" includes, volunteers, contractors, agents, and other role holders within the council including former staff*and former councillors. This also includes applicants or candidates for any of these roles.

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photograph, video, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR") and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by **Elloughton cum Brough Town Council** which is the data controller for your data.

The council works together with:

- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies

We may need to share personal data we hold with them so that they can carry out their responsibilities to the council and our community. The organisations referred to above will sometimes be "joint data controllers". This means we are all responsible to you for how we process your data where for example two or more data controllers are working together for a joint purpose. If there is no joint purpose or collaboration, then the data controllers will be independent and will be individually responsible to you.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

What data do we process?

- Names, titles, and aliases, photographs.
- Start date / leaving date
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process and referral source (e.g. agency, staff referral))
- Location of employment or workplace.
- Other staff data (not covered above) including; level, performance management information, languages and proficiency; licences/certificates, immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.
- CCTV footage and other information obtained through electronic means such as swipecard records.
- Information about your use of our information and communications systems.

We use your personal data for some or all of the following purposes: -

Please note: We need all the categories of personal data in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing any contractual benefits to you
- Liaising with your pension provider.
- Administering the contract, we have entered into with you.
- Management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Conducting grievance or disciplinary proceedings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- To undertake activity consistent with our statutory functions and powers including any delegated functions.
- To maintain our own accounts and records;
- To seek your views or comments;
- To process a job application;
- To administer councillors' interests
- To provide a reference.

Our processing may also include the use of CCTV systems for monitoring purposes.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.

We may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest or for official purposes.

How we use sensitive personal data

- We may process sensitive personal data relating to staff, councillors and role holders including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.
  - Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law.
- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

- You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

- We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.
- Less commonly, we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.
- We will only collect personal data about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

- Where appropriate, we will collect personal data about criminal convictions as part of the recruitment process or we may be notified of such personal data directly by you in the course of you working for us.

What is the legal basis for processing your personal data?

Some of our processing is necessary for compliance with a legal obligation.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

We will also process your data in order to assist you in fulfilling your role in the council including administrative support or if processing is necessary for compliance with a legal obligation.

Sharing your personal data

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with:

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to manage our HR/ payroll functions, or to maintain our database software;
- Other persons or organisations operating within local community.
- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies

- Professional advisors
- Trade unions or employee representatives

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases, the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your responsibilities

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Your rights in connection with personal data

You have the following rights with respect to your personal data: -

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. The right to access personal data we hold on you

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2. The right to correct and update the personal data we hold on you

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3. The right to have your personal data erased

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.

- When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4. ***The right to object to processing of your personal data or to restrict it to certain purposes only***
   - You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5. ***The right to data portability***
   - You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. ***The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained***
   - You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7. ***The right to lodge a complaint with the Information Commissioner's Office***
   - You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing, if we start to use your personal data for a purpose not mentioned in this notice.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on our website **www.elloughtonbrough-tc.gov.co.uk**.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints to **The Data Controller, Philippa Beverley,** in the following ways:

Address: **Elloughton cum Brough, 60 Welton Road, Brough, HU15 1BH**
Telephone: **01482 665600**
Email: **elloughtonbrough-tc.gov.uk**

Elloughton cum Brough Town Council
60 Welton Road, Brough, HU15 1BH
Write to: PO Box 124, Brough, HU15 1YH
Telephone: 01482 665600
Website: elloughtonbrough-tc.gov.uk

Privacy Policy (GDPR)

Philippa Beverley
Town Clerk

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the personal data alone or in conjunction with any other personal data. The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR) and other local legislation relating to personal data and rights such as the Human Rights Act.

Council information

This Privacy Policy is provided to you by **Elloughton cum Brough Town Council** which is the data controller for your data.

- elloughtonbrough-tc.gov.uk
- 60 Welton Road, Brough, HU15 1BH

Who are the data controllers?

- Elloughton cum Brough Town Council and East Riding of Yorkshire Council
- Community groups
- Contractors

What personal is collected?

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by a council, or where you provide them to us, we may process demographic information such as gender, age, marital status, nationality, education/work histories, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you pay for activities such as use of a council hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The data we process may include sensitive personal data or other special categories of data such as racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sex life or sexual orientation.
- Website data;
    - Information from syncing with other software or services
    - Interaction with social media
    - Information about payments
    - Access to social media profiles
    - Demographic information
- Information collected automatically from use of the service;
    - Device information (nature of device and/ or identifiers)
    - Log information (including IP address)
    - Location information
    - Device sensor information
    - Site visited before arriving

    - Browser type and or OS
    - Interaction with email messages
- Information from other sources;
    - Referral or recommendation programmes
    - Publicly accessible sources
- Information from cookies or similar technologies;
    - Essential login/authentication or navigation
    - Functionality – remember settings
    - Performance & Analytics – user behaviour
    - Advertising/retargeting
    - Any third-party software served on users
- Nature of any outbound communications with website users;
    - Email
    - Telephone (voice)

The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

We use your personal data for some or all of the following purposes:

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
- To confirm your identity to provide some services;
- To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);
- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;

- To notify you of changes to our facilities, services, events and staff, councillors and role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council, and;
- To allow the statistical analysis of data so we can plan the provision of services.

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

What is the legal basis for processing your personal data?

The council is a public authority and has certain powers and duties. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the council's statutory functions and powers. Sometime when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services. We will always take into account your interests and rights. This Privacy Policy sets out your rights and the council's obligations to you in detail.

We may also process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy.

Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

Sharing your personal data

The council will implement appropriate security measures to protect your personal data. This section of the Privacy Policy provides information about the third parties with whom the council will share your personal data. These third parties also have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases, the law imposes a time limit for such claims (for

example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data:

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

(i) The right to access personal data we hold on you
(ii) The right to correct and update the personal data we hold on you
(iii) The right to have your personal data erased
(iv) The right to object to processing of your personal data or to restrict it to certain purposes only
(v) The right to data portability
(vi) The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained
(vii) The right to lodge a complaint with the Information Commissioner's Office.

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Policy, then we will provide you with a Privacy Notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this policy

We keep this Privacy Policy under regular review and we will place any updates on our website **elloughtonbrough-tc.gov.uk**.

Contact Details

Please contact us if you have any questions about this Privacy Policy or the personal data we hold about you or to exercise all relevant rights, queries or complaints to **The Data Controller, Philippa Beverley,** in the following ways:

Address: **Elloughton cum Brough Town Council, 60 Welton Road, Brough, HU15 1BH**
Telephone: **01482 665600** Email: **elloughtonbrough-tc.gov.uk**

Elloughton cum Brough Town Council
60 Welton Road, Brough, HU15 1BH
Write to: PO Box 124, Brough, HU15 1YH
Telephone: 01482 665600
Website: elloughtonbrough-tc.gov.uk

Subject Access Request Policy (GDPR)

Philippa Beverley
Town Clerk

What must I do?

1. ***MUST***: On receipt of a subject access request you must **forward** it immediately to the **Town Clerk who is the Data Controller.**
2. ***MUST***: We must correctly **identify** whether a request has been made under the Data Protection legislation.
3. ***MUST***: A member of staff, and as appropriate, councillor, who receives a request to locate and supply personal data relating to a SAR must make a full exhaustive **search** of the records to which they have access.
4. ***MUST***: All the personal data that has been requested must be **provided** unless an exemption can be applied.
5. ***MUST***: We must **respond** within one calendar month after accepting the request as valid.
6. ***MUST***: Subject Access Requests must be undertaken **free of charge** to the requestor unless the legislation permits reasonable fees to be charged.
7. ***MUST***: Councillors and managers must ensure that the staff they manage are **aware** of and follow this guidance.
8. ***MUST***: Where a requestor is not satisfied with a response to a SAR, the council must manage this as a **complaint**.

How must I do it?

1. Notify the **Town Clerk who is the Data Controller** upon receipt of a request.
2. We must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by the council relating to the data subject. You should clarify with the requestor what personal data they need. They must supply their address and valid evidence to prove their identity. The council accepts the following forms of identification (* These documents must be dated in the past 12 months, +These documents must be dated in the past 3 months):

   Current UK/EEA Passport
   UK Photocard Driving Licence (Full or Provisional)
   Firearms Licence / Shotgun Certificate
   EEA National Identity Card
   Full UK Paper Driving Licence
   State Benefits Entitlement Document*
   State Pension Entitlement Document*
   HMRC Tax Credit Document*
   Local Authority Benefit Document*
   State/Local Authority Educational Grant Document*
   HMRC Tax Notification Document
   Disabled Driver's Pass
   Financial Statement issued by bank, building society or credit card company+
   Judiciary Document such as a Notice of Hearing, Summons or Court Order
   Utility bill for supply of gas, electric, water or telephone landline+
   Most recent Mortgage Statement
   Most recent council Tax Bill/Demand or Statement

Tenancy Agreement
Building Society Passbook which shows a transaction in the last 3 months and your address

3. Depending on the degree to which personal data is organised and structured, you will need to search emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records in relevant filing systems etc. which your area is responsible for or owns.

4. You must not withhold personal data because you believe it will be misunderstood; instead, you should provide an explanation with the personal data. You must provide the personal data in an "intelligible form", which includes giving an explanation of any codes, acronyms and complex terms. The personal data must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. You may be able to agree with the requester that they will view the personal data on screen or inspect files on our premises. You must redact any exempt personal data from the released documents and explain why that personal data is being withheld.

5. Make this clear on forms and on the council website.

6. You should do this through the use of induction, my performance and training, as well as through establishing and maintaining appropriate day to day working practices.

7. A database is maintained allowing the council to report on the volume of requests and compliance against the statutory timescale.

8. When responding to a complaint, we must advise the requestor that they may complain to the Information Commissioners Office ("ICO") if they remain unhappy with the outcome.

Sample letters

All letters must include the following information:

the purposes of the processing;

the categories of personal data concerned;

the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules[1] or EU model clauses[2];

[1]"Binding Corporate Rules" is a global data protection policy covering the international transfer of personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisation's headquarters is located. In the UK, the relevant regulator is the Information Commissioner's Office.

[2]"EU model clauses" are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.

where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

the right to lodge a complaint with the Information Commissioners Office ("ICO");

if the data has not been collected from the data subject: the source of such data;

the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Replying to a subject access request providing the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. We are pleased to enclose the personal data you requested.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely"

Release of part of the personal data, when the remainder is covered by an exemption

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. To answer your request, we asked the following areas to search their records for personal data relating to you:

- [List the areas]

I am pleased to enclose *[some/most]* of the personal data you requested. *[If any personal data has been removed]* We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you. You will notice that *[if there are gaps in the document]* parts of the document(s) have been

blacked out. *[OR if there are fewer documents enclose]* I have not enclosed all of the personal data you requested. This is because *[explain why it is exempt]*.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published, or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely"

Replying to a subject access request explaining why you cannot provide any of the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject*].

I regret that we cannot provide the personal data you requested. This is because *[explanation where appropriate]*.

[Examples include where one of the exemptions under the data protection legislation applies. For example, the personal data might include personal data is 'legally privileged' because it is contained within legal advice provided to the council or relevant to on-going or preparation for litigation. Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject. Council staff will be able to advise if a relevant exemption applies and if the council is going to rely on the exemption to withhold or redact the data disclosed to the individual, then in this section of the letter the council should set out the reason why some of the data has been excluded.]

Yours sincerely"

Elloughton cum Brough Town Council

60 Welton Road, Brough, HU15 1BH
Write to: PO Box 124, Brough, HU15 1YH
Telephone: 01482 665600
Website: elloughtonbrough-tc.gov.uk

Data Consent Form

Your privacy is important to us and we would like to communicate with you about the council and its activities. To do so we need your consent. Please fill in your name and address and other contact information below and confirm your consent by ticking the boxes below.

		If you are aged 13 or under your parent or guardian should fill in their details below to confirm their consent
Name		
Address		
Signature		
Date		

Please confirm your consent below. You can grant consent to any or all of the purposes listed. You can find out more about how we use your data from our "Privacy Notice" which is available from our website or from the Council Offices (see header).

You can withdraw or change your consent at any time by contacting the council office.

☐ **We may contact you** to keep you informed about what is going on in the Council's area or other local authority areas including news, events, meetings, clubs, groups and activities. These communications may also sometimes appear on our website, or in printed or electronic form (including social media).

☐ **We may contact you** about groups and activities you may be interested in.

☐ **We may use** your name and photo in our newsletters, bulletins or on our website, or our social media accounts (for example Facebook or Twitter).

Keeping in touch:

☐ **Yes please**, I would like to receive communications by email.
☐ **Yes please**, I would like to receive communications by telephone.
☐ **Yes please**, I would like to receive communications by mobile phone (including texts).
☐ **Yes please**, I would like to receive communications by social media.
☐ **Yes please**, I would like to receive communications by post.