Introduction

These Terms of Use and our Privacy Notice form part of our overall approach to managing Electronic Information Security.

We aim to ensure that all information held electronically and our Information Technology and Communications Services (referred to as the Services we provide) are adequately protected. Achieving this largely depends on our users working diligently in accordance with our policy guidelines.

The Services we make available to you are provided by Derby City Council. Derby City Council is the local government unitary authority for Derby City. Our address is The Council House, Corporation Street, Derby, DE1 2FS. You can contact our Data Protection Officer on 01332 640763 or by email at Data.protection@derby.gcsx.gov.uk

Neither Connect Derby or Derby City Council are the Internet Service Provider by means of whose service you will be connected to the Internet.

Questions relating specifically to the provision and operation and of the Services we provide should be directed to support@connectderby.co.uk.

How does this apply to me?

As a condition of using any of the Services we provide you must agree to abide by our Terms of Use.

You are solely responsible for all access to and use of the Services we provide including any breach of our Terms of Use by you or any user of your device. For the purposes of this Terms of Use, "you" means you and every person you authorise to use the Services we provide.

If you do not wish to be bound by our Terms of Use you may not access or use the Services we provide.

Terms of Use

The Internet may provide access to content that you or others consider harmful or inappropriate to minors, or otherwise offensive.

By using our Services, you confirm that you are either older than 18 years or have the permission of your parent or guardian to use the Services we provide.

As a condition of using the Services we provide:

You will not attempt deliberate unauthorised access to the Services we provide.

You will act lawfully and not act in any way that could be unlawful or encourage others to act unlawfully. You will not infringe intellectual property rights, reveal confidential or sensitive information and will not engage in any criminal offence or encourage others to do so.

You will act responsibly and not undertake actions that are harassing, defamatory, threatening, obscene, abusive, racist, sexist, offensive or otherwise objectionable or inappropriate.

You will not pretend to be anyone other than yourself.

You will not collect email addresses or other personal details or use the Services we provide to send spam.

You will act reasonably and not use the Services we provide in any way that may affect the operation of the Services or any other technology connected to it (for example, other users' devices).

You will act fairly and not use the Services we provide in an unreasonable or excessive manner.

You accept that sometimes, for technical, legal or operational reasons, the Services we provide may not be available.

You accept that we may control the types of material that can be sent or received over the Services we provide.

You accept that we may suspend access to the Services we provide at any time at our sole discretion without responsibility to you.

You use the Services we provide at your own risk and we are not responsible to you for any damages, losses, costs or expenses you suffer because our services are unavailable, do not operate as expected (including but not limited to download and upload speeds, bandwidth and reliability) or cause loss or damage to any data.

You accept that you are responsible to Derby City Council for all damage, losses, costs or expenses suffered by Derby City Council arising out of any breach by you of these Terms of Use.

We will investigate suspected instances of unacceptable use of the Services we provide, and this may result in our suspending your access to the Services we provide.

Where there is a risk to the security of the Services we provide, quality of service, or to order to enforce our policies, we may:

Impose restrictions on network traffic or the use of specific applications.

Refuse the connection of devices to the network.

Remove networked devices or sub-sections of the network from service.

Manage how network resources (such as bandwidth) are allocated.

What we expect from you

In general, you are expected to:

Be familiar with and comply with all our policies.

Make yourself familiar with our procedures for obtaining support.

Keep abreast of news announcements (via notices, e-mail, Web, etc.).

Keep any account details secure. Where an account is provided for individual use (for example, a where a username and password is required to access the Services we provide) you must not reveal the password or allow anyone else to use that account.

Privacy Notice

We rely on our contractual arrangements with you as the lawful basis on which we collect and process your personal data. This data is used to:

Manage your access to and use of the Services we provide.

Identify or investigate operational problems with the Services we provide to you and to monitor for their correct operation.

Investigate suspected unauthorised access to or use of the Services we provide.

Identify and control security threats including defending against attacks against our systems or the Services we provide.

Support the detection or prevention of activities that are in breach of our policies.

Comply with legislation.

We routinely monitor and log user-specific information including:

Device information. This includes information about devices accessing the Services we provide. This may include type of device, what operating system is used, device settings, application IDs, unique device identifiers (including Internet Protocol address) and MAC addresses. Whether we collect some or all of this information often depends on the type of device used and its settings.

Location Analytics. To better understand user behaviour, we capture location analytics data. We do this by capturing and analysing the beacons that every WiFi enabled device periodically emits when its WiFi is turned on to detect the presence of nearby wireless networks whether they join the network or not. Location Analytics distinguishes between devices and recognizes repeat visitors by collecting a MAC address. Only a device's MAC address is captured, and the aggregated data provided cannot be traced back to an individual without our having prior knowledge of the MAC address of the device. Our location analytics platform uses a one-way hash function to anonymize MAC addresses before storage. The function is irreversible; given a specific hashed MAC, there is no way the function can be

undone to reveal the original MAC address. In addition, bytes are dropped from the hashcode, meaning that even if we knew the hash function, we could not determine if a specific MAC had visited a location.

Content (web) Filtering. When you use the Services we provide to access the Internet we may (in an attempt to minimise the risk of exposure to material that is illegal or may be regarded as inappropriate or unacceptable) screen traffic by means of a Content (web) Filter. This will record the address or URL of any webpage that you try to access, the words entered into a search engine and the fact that an attempt to access a restricted site has been made. In addition, some features of our Content (web) Filtering platform do involve the use of profiling, for example, we receive alerts when a user exceeds certain thresholds, such as trying to access pornographic sites more than 10 times. However, no automated decisions for the purposes of GDPR are made.

Monitoring and logging the use of the Services we provide is only undertaken by specific members of Derby City Council staff as a recognised part of their normal duties.

Securing your personal data

We have put in place appropriate security measures to reduce the risk of your personal data being accidentally lost, altered, disclosed, used or accessed in an unauthorised way.

We limit access to your personal data to specific Derby City Council staff and third-parties who have a business need to know. They will only process your personal data in accordance with our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and the regulator of a breach where we are legally required to do so.

Retaining your personal data

We will only retain your personal data for as long as necessary for the purposes described in this Privacy Notice. This means that the retention periods will vary according to the type of the data and the reason that we have the data in the first place.

When we determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

We may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

Subprocessors

Where we do not have the capability to provide certain services ourselves we work with several suppliers (our subprocessors) who provide these services on our behalf. In each case, the supplier is only allowed to use your personal data to provide services to us and for no other purpose.

These subprocessors include:

Cucumber Tony who provide our WiFi Captive Portal. Data is stored in the European Economic Area (EEA).

CISCO Meraki who provide WiFi Analytics and Network Management tools. Data is stored in the EEA.

CISCO who provide WiFi Analytics and Network Management tools. Data is stored in the EEA.

Amazon Web Services who host our Radius authentication. Data is stored in the EEA.

Zoho Corporation who provide our Helpdesk and CRM systems. Data is stored in the EEA.

Transfer of your personal data outside the EEA

We may need to transfer your personal data outside of the European Economic Area (EEA), for example, to the USA. Where we work with a supplier who processes personal data outside of the EEA we will make sure that any transfer of your personal data is subject to appropriate safeguards and is treated as if it were being processed inside the EEA under the principles set out in this Privacy Notice.

How we share and disclose information

We will comply with a request for information if we reasonably believe disclosure is in accordance with or required by any applicable law, regulation or legal process. We will not sell or rent your information to third parties. We will not share your information with third parties for marketing purposes.

Your Rights

You can read more about your rights in the guidance provided by the Information Commissioner's Office (ICO) https://ico.org.uk/for-the-public. You have the right to complain about our use of personal data to the ICO and can do this by contacting the ICO via their website https://ico.org.uk/concerns, or by calling 0303 123 1113.

Changes to Terms of Use and Privacy Notice

We may update our Terms of Use and Privacy Notice from time to time. If we make significant changes we will let you know but please regularly check this policy to ensure you are aware of the most updated version.

Complaints

If you would like to make a compliant regarding the use of your personal data you can contact our Data Protection Officer; By Post: Information Governance The Council House, Corporation Street, Derby, DE1 2FS By phone: 01332 640763 By email: Data.protection@derby.gcsx.gov.uk

Our Terms of Use and Privacy Policy were last updated on 12 June 2018.