Changes to Data Protection legislation
Assurance statement

This document describes Nottingham CityCare Partnership's (CityCare) compliance against changing data protection legislation: General Data Protection Regulation (GDPR) in force from 25 May 2018 and supporting domestic legislation in Parliament at the time of writing. You can find out more about the changes from the Information Commissioner's Office website at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

Compliance with legislation is an ongoing and business as usual process. The size and complexity of CityCare's organisation and operations means that large numbers of partners and stakeholders are seeking assurance, and this general statement has been derived from the Information Commissioner's Office checklist for data controllers, available from the ICO's website.

CityCare demonstrates compliance with existing law through the NHS Digital Information Governance Toolkit. Reporting is available to the general public from https://www.igt.hscic.gov.uk/ (click on reporting from the left-hand menu and use organisation code NR3 to search). The IG Toolkit for 2017-18 (v14.1) had a final outcome of Satisfactory. From 2018-19, assurance will be provided through the NHS Digital Data Security & Protection Toolkit and Care Quality Commission (CQC) reporting.

CityCare is a social enterprise, not a public authority, and is therefore not subject to the Freedom of Information Act (2000). We do want to be transparent about our activity and obligations, so if further detail is required, please contact ncp.customercare@nhs.net with a copy to your main CityCare contact, as we will need to work with them to provide you with a response. We may need to forward your request to partner organisations if they are better placed to answer your questions and will contact you to discuss if this is necessary. Thank you.

Compliance statement

Lawfulness, fairness and transparency	
Personal information held, processing activities and legal basis (including consent)	• Please see CityCare's Privacy Notice at https://www.nottinghamcitycare.nhs.uk/stakeholders/governance/you-and-your-information/ and in bedside folders. This notice is currently being updated, and will include information for staff and other stakeholders. • The legal bases for processing rely on GDPR itself, relevant health and social care legislation, employment legislation and/or consent, as appropriate to the circumstances. Many of these are in place at present for compliance with existing legislation. • CityCare does not provide online services for children.
Registration with the Information Commissioner's Office	• Z2602430
Individuals' rights	
Right to be informed	• Privacy Notice in place and under update, as above. • Information already provided to individuals on an 'as needs' basis, for example, when referrals are made to another service, public health information. • 'Child friendly' information is under development.
Right of access	• Processes are in place for individuals to request access to their records. See Privacy Notice for details of processes. Work is in progress to implement updated procedures for compliance with changes in new legislation.
Right to rectification and data quality	• Already part of business as usual processes. See Information Governance Toolkit requirements relating to data quality.

	• The NHS Care Records Guarantee provides for correction of errors in care records, and the right for individuals to contribute to their own records.
Right to erasure including retention and disposal	• The right to erasure does not apply to health or employment records, where CityCare's legal obligations to process personal data for defined periods of time over-ride the right to erasure. • The right to erasure may apply to other types of personal information, such as contact details for mailing about news and events. Please contact the sender directly about these. • Records are retained in accordance with the national Records Management Code of Practice for Health & Social Care, which can be found at https://digital.nhs.uk/records-management-code-of-practice-for-health-and-social-care-2016. Note: The Independent Inquiry into Child Sexual Abuse requires health and social care providers, including CityCare, to retain some records indefinitely. Please see the Inquiry's website for details of records in scope at https://www.iicsa.org.uk.
Secure disposal	• All confidential paper waste is securely shredded on site. • All devices are securely disposed by Nottinghamshire Healthcare Informatics Services (NHIS), which is hosted by Sherwood Forest NHS Foundation Trust and provides IT services for CityCare. • NHS Standard Contracts for Provision of Goods & Supply of Services apply to all sub-contractors, ensuring that they are working to the appropriate security standards.
Right to restrict processing; Right to object to processing	• The right to object to, or restrict processing only applies where this right over-rides CityCare's numerous legal obligations to process personal data for defined periods of time in order to comply with other legislation (health and social care legislation; employment law). A list of the most frequent relevant legislation is appended to this document. • For care records, it is important to note that the increasing nature of multi-agency care provision means that objecting to, or restricting sharing of records between care providers

	may have a negative impact on an individual's care. Patients are advised that they should discuss any restrictions with the relevant care provider and understand any implications for their care if they wish to restrict or object to processing. • CityCare's primary patient administration and records system is SystmOne, which has the function to permit or prevent sharing of clinical care information. SystmOne is in wide use throughout the NHS.
Right of data portability	• For care records, this is already in place via transfers of care arrangements when an individual changes providers. • This right is under review in relation to provision of copies of records (right of access) and other types of information and is believed to be limited in a statutory setting, given legal obligations and bases for data processing outlined in other areas of this document.
Rights related to automated decision making including profiling	• This activity is not commonly undertaken within CityCare: decisions about individuals' care are undertaken by the relevant clinical staff. • All organisations that provide health and social care services also have duties to improve services and contribute to public health population improvements. These mean that some automated profiling activity takes place on personal information for analytical and planning purposes only: no decisions are made about individuals specific needs for care, and all identifiable information is removed from reporting.
Accountability and governance	
Policies	• CityCare has a full range of Information Governance policies, procedures and guidance for staff. These are being updated to take changed legislation into account.
Monitoring of compliance; Information Risk Management; Management Responsibility	• CityCare has robust governance processes in place: an Information Governance sub-committee meets monthly and reports to the Finance & Performance Committee of the Board. The Senior Information Risk Owner (SIRO) provides reports to the Board on a quarterly basis.

	• CityCare's SIRO is the Director of Finance. The Director is an Executive Member of the Board and chairs the Information Governance sub-committee. Risks are a standing item on the sub-committee's agenda, including cyber-security risk. •
Your business provides data protection awareness training for all staff	• In place: annual training for staff has been mandated within the NHS since 2006-7 to national standards, updated from time to time. Information about current programmes and standards are available at https://www.e-lfh.org.uk/programmes/. • Assurance is provided through NHS Digital and CQC reporting – see above.
Data processor contracts	• All procurement of goods and services is based on the NHS Standard Contract for Provision of Goods and Supply of Services, available at https://www.gov.uk/government/publications/nhs-standard-terms-and-conditions-of-contract-for-the-purchase-of-goods-and-supply-of-services. This includes data protection compliance clauses for all suppliers. • Sharing agreements with other organisations, for example, other providers of health and social care, are supported by an over-arching multi-agency sharing protocol where signatory organisations declare that they are compliant with confidentiality and data protection standards. This has been made publicly available by the Nottinghamshire Safeguarding Board and can be found here: http://nottinghamshirescb.proceduresonline.com/files/info_sharing_pr.pdf
Data Protection by Design; Data Protection Impact Assessments; DPIA framework	• Data Protection Impact Assessments (formerly Privacy Impact Assessments) are part of business case and new project planning documentation. • Completion of impact assessments is also requested for clinical audits or other non-procurement activity. • Research ethics processes include DPIA principles in relation to privacy and information security.

	• All PIAs are reviewed by the Information Governance team, and progressed to CityCare's Caldicott Guardian if senior clinical review and signoff is required, and additionally to the SIRO for higher risk or large scale projects. • CityCare's Board and committees receive regular reporting and assurance about all organisational activity.
Data Protection Officer	• CityCare's Data Protection Officer is currently the CEO, this will change following recruitment process .Confirmation will be provided once this process is completed.
Data security, international transfers and breaches	
Information Security Policy	• CityCare has a full range of Information Governance policies, procedures and guidance for staff, which include information (data) security. • These are being updated to take changed legislation into account.
International transfers	• CityCare does not transfer any personal data outside the EEA as part of its regular service provision. • CityCare's duties to monitor and improve services mean that some identifiable data may be extracted from our records systems for analysis by external organisations. When our commissioners ask us to participate in health improvement projects. These organisations do not have any other access to your records and are under strict obligations of confidentiality and information security. • Information may be transferred to overseas patients, or their nominated representatives at an individual request level, for example, relatives or overseas healthcare providers. Emails are encrypted and individuals advised that information that leaves NHS networks may not be secure. The legal basis for this processing is consent.
Breach notification	• Reporting of personal data breaches follows CityCare's regular incident reporting processes. Higher level breaches are notified immediately to the Caldicott Guardian and/or Senior Information Risk Owner for external reporting as required by existing NHS incident reporting

	frameworks. • Information incident statistics are reported to the Information Governance sub-committee.