Veritau Group

Information Security Policy

Contents

PURPOSE AND OBJECTIVES

1 The policy gives effect to that principle of the UK GDPR which requires the Group to protect the personal data which it processes against unauthorised or unlawful processing and against accidental loss, destruction or damage by implementing appropriate technical and organisational measures.

2 This policy should be read in conjunction with the other policies in the Group's policy framework with particular focus on the Acceptable Use Policy and the Information Security Incident Reporting Policy.

SCOPE

3 All policies in the Information Governance policy framework apply to all Group employees, any authorised agents working on behalf of the Group, including temporary or agency employees, and third party contractors. Obligations on Group employees, set out below, apply equally to all such individuals.

4 Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

5 The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs, videos and other digital images.

ACCESS CONTROLS

6 Access controls will be appropriate to the format of the data, the risks applicable to it, and the role of the individual accessing the data.

Manual Filing Systems

7 Access to manual filing systems will be controlled by a key management system. All files that contain personal data will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use.

8 Keys to storage units will be stored securely (eg in a key-safe). Where used, any password or numeric entry code will be changed every three months.

Electronic Systems

9 City of York Council hosts the Group's principal databases, including Galileo, InCase, WorkPro, Xero and others. It also provides a range of desk-top applications (eg Outlook, Teams, Excel and Word), used as business tools and generating business records stored on CYC servers. Access to, and use of, all of these is governed by CYC security standards.

10 Some business functions, including payroll and HR, are hosted by North Yorkshire County Council. Access to, and use of, all of these is governed by NYCC security standards.

11 NYCC permits access to its network and service functions to allow the Group to carry out its services to NYCC as a client. Other client councils provide similar access to their own networks. Access to, and use of, each of these is governed by that client's security standards.

12 This policy requires Group employees to abide by all host and client council security standards, including two-or-more-factor authentication mechanisms, changing passwords, password strength, and maintaining password secrecy.

Security Classifications

13 The Group will have regard to the policies and practices applicable to each client in respect of security classifications. The Group will not routinely mark information relating to a client unless a security classification scheme is in place. Similarly, the Group will not mark its own documents.

14 The above standards are a minimum. This policy provides for additional electronic and other security controls as follows.

15 Access to the Group's principal databases is limited to employees in those branches of the business to which they relate:

Internal Audit	Galileo
Counter-fraud	Opus
Information Governance	WorkPro
Administration and Management	Xero, MyView and related databases; plus some admin functions in WorkPro and Opus

16 CYC provides server storage to the Group in a way which permits the Group to subdivide its storage segment. This segment is to be structured in accordance with the Group's Records Management Policy, and applying security controls such that one sub-segment is accessible only to Management, and another to nominated senior managers. The remainder is accessible to all employees.

17 The following sections set out non-technical measures to control (ie reduce) access in finer detail.

18 An individual's username, and hence access, will be suspended if that individual is suspended for disciplinary reasons or leaves the employment of the Group[1].

[1] Responsibility for this lies with the relevant Information Asset Owner but must be triggered by the disciplinary or exit procedure

Software and Systems Audit Logs

19 The Group will ensure that its principal software and systems have inbuilt audit logs so that the Group can monitor what employees and users have accessed and what changes may have been made. Although this is not a preventative measure it does ensure that the integrity of the data can be assured and also deters individuals from accessing records without authorisation.

Data Shielding

20 The Group does not allow employees to access the personal data of family members or close friends. Employees becoming aware that family or others are the subject of investigation or other processing within the group should report the relationship to their line manager and recuse themselves from that work.

21 The Group will then keep paper files in a separate filing cabinet (with access restricted to minimal employees) and where possible any electronic files will be locked down so that the declaring employee cannot access that data.

22 Employees who knowingly do not declare family and friends in such circumstances may face disciplinary proceedings and may be investigated under Section 170 of the Data Protection Act 2018 (unauthorised access to information).

PHYSICAL SECURITY

23 At offices or other accommodation provided by a host council, or by any client, all its security measures must be observed as a minimum. In addition the following provisions apply.

24 Group employees will not leave personal data on desks, or any other working areas, unattended and will use the lockable storage units provided to secure personal data when not in use.

25 When temporarily leaving a workstation it will be locked (ie screen blanked, using CTRL+ALT+DEL or WIN+L) and re-opened on return. Paper documents will be turned face down.

26 Conversations which may include discussion of personal data will be conducted in a way that avoids unauthorised persons overhearing what is said. Closing doors or moving to a separate room may be appropriate, especially if individuals not bound by this policy may overhear. Group employees overhearing personal data will ignore it and make no record of what they have learned.

Visitor Control

27 Visitors to the Group will be required to sign in a visitor's book and state their name, organisation, and nature of business. This may be in either paper or electronic format and may be completed by host council reception staff. Visitors will be escorted throughout their visit and will not be allowed to access restricted areas without Group employee supervision.

SYSTEMS SECURITY

28 Group employees must request authorisation from City of York IT (or other host or client council) before downloading software, or photos, videos, music, games or other files onto its network or onto a mobile phone provided by it. See above for conformity to CYC (or other host council) security standards.

Shared Drives

29 Technical access controls over the Group's shared server segment permit all employees to access sub-segments relating to business areas to which they do not belong. Imposing technical constraints introduces inefficiencies and anomalies, and restricts flexibility in sharing or re-assigning employees or tasks, and is minimised for this reason. Too close restrictions on access to physical locations (such as filing cabinets) are also likely to have unintended consequences.

30 Therefore the general permission to access records or documents is available only when there is an authorised (or authorisable) business need for the employee concerned to do so. Browsing or searching for, or opening or accessing, any record or document without a demonstrable business need to do so is a breach of this policy.

COMMUNICATIONS SECURITY

Social engineering attacks

31 The Group will keep its employees informed of security risks posed by social engineering tactics, such as phishing emails, whaling, pretexting, or baiting, with advice on avoiding them.

32 Group employees will not to click on links that have been sent to them in emails when the source of that email is unverified. Employees will check with CYC IT if they are unsure about the validity of an email.

33 When communicating on behalf of a client by post or email, that client's security measures will apply. Where these require checks or double-checks, these will be carried out diligently.

34 Subject to the above, security measures applied to communications will be appropriate to the sensitivity of the personal data included, and to the risk of unauthorised disclosure or processing.

Sending Personal Data by post

35 When sending personal data, by post, the Group will use Royal Mail's standard postal service. Employees will double check addresses before sending and will ensure that the envelope does not contain any data which is not intended for the addressee.

Sending Special Category Data by post

36 When sending special category data by post the Group will use Royal Mail's Recorded delivery postal service. Employees will double check addresses before

sending and will ensure that the envelope does not contain any data which is not intended for the addressee. If the envelope contains information that is thought to be particularly sensitive then employees are advised to have the envelope double checked by a colleague.

Sending Personal Data and Special Category Data by email

The Group will only send personal data and special category data by email if using a secure email transmission portal such as Egress. Where the intended recipient will not accept such emails (eg ICO or Home Office) then a password-protected attachment will be used. Alternatively such an addressee may be asked to take responsibility for the insecurity of email in the public internet.

37 The above measures are not necessary for emails sent within the NYnet secure "tunnel". This includes emails to and from NYCC.

38 Employees will always double check the recipient's email address to ensure that the email is being sent to the intended individual(s).

Exceptional Circumstances

39 In exceptional circumstance the Group may wish to hand deliver, or use a direct courier, to ensure safe transmission of personal data. This could be because the personal data is so sensitive that the usual transmission methods would not be considered secure, or because the volume of the data that needs to be transmitted is too big for usual transmission methods.

Using the BCC function

40 When sending emails such that it would be a breach of their privacy for recipients to know each other's email addresses then Group employees will use the Blind Copy (BCC) function.

REMOTE AND HOME WORKING

41 The risks involved in working at home, and appropriate and effective mitigations, and Group support (including financial support) for those mitigations, are to be discussed by each employee and his or her line manager at least twice per year. The record of this discussion may be presented during the investigation of a security breach.

42 Employees will not leave or store personal data or Group equipment in an unattended car.

Private Working Area

43 Employees will not work with personal data in areas where other individuals could potentially view or even copy the personal data (for example on public transport).

44 Employees will take care to ensure that other household members do not have access to the Group's personal or business data; and will not use Group equipment for their personal purposes.

Trusted Wi-Fi Connections

45 Employees will only connect their devices to trusted Wi-Fi connections and will not use 'free public Wi-Fi' or 'Guest Wi-Fi'. This is because such connections are susceptible to malicious intrusion.

46 When using home Wi-Fi networks employees should ensure that they have appropriate security, anti-virus software and firewalls installed to safeguard against malicious intrusion. If in doubt employees should seek advice from the Group.

Encrypted Devices and Email Accounts

47 Employees will only use Group issued encrypted devices to work on personal data. Employees will not use their own personal devices for storing, or creating personal data. This is because personal devices do not possess the same level of security as a Group issued device.

48 Employees will not use personal email accounts to access or transmit Group personal or business data. Employees must only use Group issued, or Group authorised, email accounts.

Data Removal and Return

49 Employees will only take personal data away from the Group premises if this is required for a genuine business need. Employees will take care to limit the amount of data taken away from the premises.

50 Employees will ensure that all documents and records are returned to Group premises for either re-filing or safe destruction. Employees will not destroy data away from the premises as safe destruction cannot be guaranteed.

COMPLIANCE

51 Employees are required to comply with this policy. Failure to do so may result in disciplinary action being taken.

REVIEW AND REVISION

52 This policy will be reviewed annually.

REFERENCES

53 This policy should be read in the context of the Group's other information governance policies and guidelines, national legislation and codes of practice, and accepted best practice.

54 The following policy documents are directly relevant to this policy:

- Information Governance Policy
- Records Management Policy
- Data Protection Policy

KEY MESSAGES

55 facilities provided by clients for working with personal data (including IT devices or networks, filing systems, or office accommodation) are subject to that client's security requirements as a minimum.

56 Personal data being processed on behalf of a client is subject to that client's security requirements, including its incident reporting procedure, as a minimum.