Information Security Policy 2021-22

Lead Responsible:	Data Protection Officer
Approval Dates for Revisions:	
Equality Impact Assessment	
Audit Committee	
Governing Body	
Effective Date:	4 February 2019
Annual Review Date:	
Original Filename:	Z:\Data Protection\Policies-Process\Information Security Policy 2019-20.docx

Introduction

1. The College is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

2. In relation to personal information, under Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), the College will:

    a) use technical or organisational measures to ensure personal information is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;

    b) implement appropriate technical and organisational measures to demonstrate that it has considered and integrated data compliance measures into the College's data processing activities; and

    c) be able to demonstrate that it has used or implemented such measures.

3. This purpose of this policy is to:

    a) protect against potential breaches of confidentiality;

    b) ensure all our information assets and IT facilities are protected against damage, loss or misuse;

    c) support the College's Data Protection Policy in ensuring all staff are aware of and comply with UK law and the College's procedures applying to the processing of personal information; and

    d) increase awareness and understanding in the College of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they themselves handle.

4. The College will review and update this policy in accordance with our obligations. This policy does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

5. If you have any questions regarding this policy, please contact the Data Protection Officer.

Definitions

6. For the purposes of this Policy:

business information	means business-related information other than personal information regarding customers, clients, suppliers and other business contacts of the College;
confidential information	means trade secrets or other confidential information (either belonging to the College or to third parties) that is processed by the College;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

Roles and responsibilities

7. Information security is the responsibility of all staff. The College's Data Protection Officer (DPO) is in particular responsible for:

   a) monitoring and implementing this policy;

   b) monitoring potential and actual security breaches;

c) ensuring that staff are aware of their responsibilities; and

d) ensuring compliance with the requirements of Regulation (EU) 2016/679, GDPR and other relevant legislation and guidance.

Scope

8. The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the College, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.
9. This policy applies to all staff, including employees, temporary and agency workers, other contractors, interns, volunteers and apprentices.

10. All staff must be familiar with this policy and comply with its terms.

11. The College information covered by this policy may include:

    a) personal information relating to staff, customers, clients, suppliers;

    b) other business information; and

    c) confidential information.

12. This policy supplements the College's Data Protection Policy, privacy notices and other policies and the contents of those documents must be taken into account in addition to this policy.

General principles

13. All College information must be protected from loss, theft, misuse or inappropriate access or disclosure.

14. Personal information, and sensitive personal information, must be protected against unauthorised and/or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical and organisational measures.

15. Staff should discuss with line managers the appropriate security arrangements and technical and organisational measures which are appropriate and in place for the type of information they access in the course of their work.

16. College information (other than personal information) is owned by the College and not by any individual or team.

17. College information must be used only in connection with work being carried out for the College and not for other commercial or personal purposes;

18. Personal information must be used only for the specified, explicit and legitimate purposes for which it is collected.

Information management

19. Personal information must be processed in accordance with:

    a) the data protection principles, set out in the College's Data Protection Policy;

    b) the College's Data Protection Policy generally; and

    c) all other relevant policies.

20. In addition, all information collected, used and stored by the College must be:

    a) adequate, relevant and limited to what is necessary for the relevant purposes;

    b) kept accurate and up to date.

21. The College will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage, including:

    a) pseudonymisation of personal information;

    b) encryption of personal information;

    c) password protected system access;

    d) system security measures including firewall, anti-virus, anti-malware

    e) regular mandatory staff training on IT security and GDPR

22. Personal information and confidential information will be kept for no longer than is necessary and stored and destroyed in accordance with the College's records retention policy.

Human resources information

23. Given the internal confidentiality of personnel files, access to such information is limited to [the HR Department]. Except as provided in individual roles, other staff are not authorised to access that information.

24. Any staff member in a management or supervisory role or involved in recruitment must keep personnel information strictly confidential.

25. Staff may ask to see their personnel files and any other personal information in accordance with Regulation (EU) 2016/679, GDPR and other relevant legislation. For further information, see the College's data subject access request policy.

Access to offices and information

26. Office doors, keys and access codes must be kept secure at all times and keys or access codes must not be given or disclosed to any third party at any time.

27. Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by, e.g through office windows.

28. Visitors must be required to sign in at reception, accompanied at all times and never left alone in areas where they could have access to confidential information.

29. Wherever possible, visitors should be seen in meeting rooms. If it is necessary for a member of staff to meet with visitors in an office or other room which contains College information, then steps should be taken to ensure that no confidential information is visible.

30. At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing confidential information must be securely locked away.

Computers and IT

31. Password protection and encryption will be used where available on College systems in order to maintain confidentiality.

32. Computers and other electronic devices will be password protected and those passwords must be changed on a regular basis. Passwords must not be written down or given to others.

33. Computers and other electronic devices will be locked when not in use and when you leave your desk, to minimise the risk of accidental loss or disclosure.

34. Confidential information must not be copied onto removable hard drive, CD, DVD or memory stick/ thumb drive without the express permission of the Data Protection Officer. Data held on any of these devices should be transferred to the College's computer network as soon as possible in order for it to be backed up and then deleted from the device.

35. All electronic data will be securely backed up at the end of each working day in line with the College IT Security Policy.

36. Staff must ensure they do not introduce viruses or malicious code on to College systems. Software must not be installed or downloaded from the internet. Staff should contact IT Services for guidance on appropriate steps to be taken to ensure compliance.

Communications and transfer of information

37. Staff must be careful about maintaining confidentiality when speaking in public places, e.g when speaking on a mobile telephone.

38. Confidential information must be marked 'confidential' and circulated only to those who need to know the information in the course of their work for the College. Further details of how emailed information must be marked and protected are set out in the rest of this policy.

39. Confidential information must not be removed from the College's offices unless required for authorised business purposes, and then only in accordance with paragraph 40 below.

40. Where confidential information is permitted to be removed from the College's offices, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained. Staff must ensure that confidential information is:

    a) stored on an encrypted device with strong password protection, which is kept locked when not in use;

    b) when in paper copy, not transported in see-through or other unsecured bags or cases;

    c) not read in public places (e.g waiting rooms, cafes, trains); and

    d) not left unattended or in any place where it is at risk (e.g in conference rooms, car boots, cafes).

41. Postal, document exchange (DX) and email addresses and numbers should be checked and verified before information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

42. All sensitive or particularly confidential information should be encrypted before being sent by email, or be sent by tracked DX or recorded delivery.

Personal email and cloud storage accounts

43. Personal email accounts and cloud storage services are vulnerable to hacking. They do not provide the same level of security as the services provided the College IT systems.

44. Do not use a personal email account or cloud storage account for work purposes.

45. If you need to transfer a large amount of data, contact IT Services for help.

Home working

46. Staff must not take College information home unless required for authorised business purposes and then only in accordance with paragraph 47 below.

47. Where staff are permitted to take College information home, staff must ensure that appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information. In particular:

    a) personal and confidential information must be kept in a secure and locked environment where it cannot be accessed by family members or visitors; and

    b) all personal and confidential information must be retained and disposed of in accordance with paragraph 22 above.

48. Staff must not store confidential information on their home computers (PCs, laptops or tablets).

Transfer to third parties

49. Third parties should be used to process College information only in circumstances where appropriate written agreements are in place ensuring that those service providers offer appropriate confidentiality,

information security and data protection undertakings. Consideration must be given to whether the third parties will be processors for the purposes of Regulation (EU) 2016/679, GDPR.

50. Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the Data Protection Officer for more information.

Overseas transfer

51. There are restrictions on international transfers of personal information. Staff may only transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway, with the prior written authorisation of the Data Protection Officer.

52. You should refer to the College's data protection policy for further information on overseas transfers.

Training

53. All staff will receive training on GDPR and IT security as appropriate.

54. Completion of training is compulsory.

55. The Data Protection Officer will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or our Information management and security policy or procedures, please contact the Data Protection Officer.

Reporting breaches

56. All members of staff have an obligation to report actual or potential data protection compliance failures. This allows the College to:

    a) investigate the failure and take remedial steps if necessary;

    b) maintain a register of compliance failures; and

    c) make any applicable notifications.

57. Please refer to the College Data Breach Policy and Data Breach Notification Procedure for details on what constitutes a data breach and the procedures to follow to report such a breach.

Consequences of failing to comply with this policy

58. The College takes compliance with this policy very seriously. Failure to comply with it puts both staff and the College at significant risk. The importance of this policy means that failure to comply with any requirement of it may lead to disciplinary action, which may result in dismissal.

59. Staff with any questions or concerns about anything in this policy should not hesitate to contact the DPO.