To request a copy of this document in an alternative format such as large print, please contact 01922 657014

1 Introduction

1.1 This Policy;

1.1.1 places obligations on staff to comply with the provisions of the Data Protection Act 2018, the General Data Protection Regulations (GDPR) and any other related legislation relating to the protection and free movement of personal data.

and

1.1.2 set out the College's commitments and responsibilities for processing personal data.

1.2 Scope

This Policy applies to all staff including employees, contractors, agency staff and other persons working for Walsall College, and to all Personal Data and Special Category (sensitive) Personal Data held by the College. This Policy should be read in conjunction with the Data Breach Plan, E-Communications Policy and related policies. These provide a more detailed guide on the handling of personal data.

The Policy sets out how Walsall College will ensure that it is compliant with the requirements of the Data Protection Act 2018 and all other related data protection legislation and guidance.

1.3 The aim of this Policy is to provide staff and customers with information about the College's approach to Personal Data and assurance of compliance.

1.4 Walsall College ('the College') needs to keep Personal Data about its employees, students and users to allow it to monitor performance, achievements, and health and safety. It is also necessary to process Personal Data so that staff can be recruited and paid, courses organised and to comply with legal obligations to funding bodies and government. To comply with the law, Personal Data must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

1.5 The College is registered with the Information Commissioners Office (ICO), our registration number is Z5015525.

2 Definitions

Data Controller: Walsall College is the Data Controller and this means it determines the purposes and means of the processing of Personal Data.

Personal Data Breach: means a breach of information security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, which is transmitted, stored or processed in any other way. This includes breaches that are the result of both accidental and deliberate causes. Personal Data Breaches can lead to compromises of Confidentiality, Integrity, and or Availability.

Information Commissioner's Office (ICO): means the UK's independent data protection and information regulator.

Personal Data: means any information relating to an identifiable living person who can be directly or indirectly identified in particular by reference to an identifier. Individuals can be students, contractors, alumni, former employees, job applicants, agency, contract and other staff, suppliers and marketing contacts. Personal Data can include expression of opinion about the individual and any indication of someone else's intentions towards the individual. Personal Data includes 'Special Category Personal Data', which was previously known as Sensitive Personal Data.

Special Category Personal Data: means Personal Data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health condition, sexual life and sexual orientation, genetic, biometric data and criminal offences, or related proceedings.

GDPR: means General Data Protection Regulation, it is designed to harmonize data privacy laws across Europe, to protect and empower individuals and reshape the way organisations approach data privacy.

3 The Data Protection Principles

The College must comply with all data protection legislation and in particular the Data Protection Principles, which are currently set out in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. In summary, these state that Personal Data shall be:

a) Processed lawfully, fairly and in a transparent manner.
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purpose.
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d) Accurate and kept up to date; inaccurate Personal Data will be erased or rectified without undue delay.
e) Not kept for longer than is necessary for the purpose for which the Personal Data are processed.
f) Kept secure against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The legislation also require that the College must be responsible for demonstrating how it complies with the principles. The fully expanded principles are set out at Appendix 1.

The College, its staff and all others who process or use Personal Data, including third parties who process Personal Data on the College's behalf, must ensure that they follow these principles at all times.

4 Individual Rights

4.1 All staff, students and other users have:

1. a right to be informed of what information the College holds and processes about them and why.
2. a right to gain access to this information (Subject Access Request)
3. a right to have Personal Data corrected where it is inaccurate or incomplete
4. a right to have Personal Data erased in certain circumstances
5. a right to restrict how Personal Data is processed or used in certain circumstances

6. a right to obtain and reuse their Personal Data for their own purposes across different services, in certain circumstances
7. a right to object to the use of Personal Data for marketing, specific research and public interest purposes
8. a right to know if the college is using their personal data to carry out solely automated decision-making or profiling that has legal or similarly significant effects on them.

5 Exemptions to Exercise of Individual Rights

5.1 A small number of specific activities are exempt or subject to conditions or rules, these include processing that relates to:

5.1.1 Subject Access Requests relating to information about the outcome of academic, professional or other examinations. These rules, which apply to requests for examination scripts, marks or markers' comments, are designed to prevent the right of subject access being used as a means of circumventing an examination body's processes for announcing results.

5.1.2 Personal Data used for archiving, scientific or historical research or statistical purposes.

5.1.3 Exemptions or rules may apply where there is a need to protect the individual, or the rights and freedoms of others for the prevention, investigation, detection or prosecution of criminal offences;

5.1.4 Other exemptions that are available are of a very specific nature. They relate to matters such as National Security, Crime and Taxation, Health, judicial independence and proceedings, or breaches of ethics in regulated professions matters

If you would like to exercise your rights, please visit our Individual Rights page at www.walsallcollege.ac.uk.

6 Lawful Basis for Processing Personal Data

- The College must have a valid lawful basis in order to process Personal Data.
- There are six available lawful basis for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the activity purpose and relationship with the individual.
- Most lawful basis require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you will not have a lawful basis.
- The College must determine the lawful basis before it begins processing, and should document it in the College Information Asset Register (Records of Processing Activity).
- Walsall College Privacy Notices should include the lawful basis for processing as well as the purposes of the processing.

- If processing purposes change, staff may be able to continue processing under the original lawful basis if the new purpose is compatible with the initial purpose (unless the original lawful basis was consent).

- Where the College is processing Special Category Personal Data, we must identify **both** a lawful basis for general processing and **an additional condition** for processing this type of data.

If the College is processing criminal conviction data or data about offences, staff need to identify **both** a lawful basis for general processing and an additional condition for processing this type of data.

In some cases, we will also have an 'appropriate policy document' in place to rely on these conditions.

7 Consent

7.1 Consent is one of the conditions that Walsall College can rely upon to justify processing Personal Data, but it is not the only one. In many cases, there will be another justifiable lawful reason and consent will not be required. All processing of Personal Data must be based on one of the lawful condition or bases. Please see the guidance on lawful basis and consent at Appendix 2.

7.2 In instances where consent is given as the primary fair processing condition, individuals may choose to withdraw their consent by sending an email to gdpr@walsallcollege.ac.uk or requests can be submitted in writing using the Consent Withdrawal form at Appendix 3. However, where the College has other lawful basis of processing Personal Data, it will continue to do so.

8 Records of Processing Activity (Information Asset Register)

8.1 Detailed records of the purposes we process personal data, when and how we share Personal Data and our retention policies must be kept. This means that all computerised Personal Data and structured manual data files retained by the College must be recorded by Information Asset Owners and provided to the Data Protection Officer who will ensure compliance with the College's Data Protection Policy and the Act.

8.2 Information Asset Owners must conduct regular reviews of these Records of Processing Activity and update our records accordingly.

9 Data Security

9.1 The College takes information security very seriously and has security measures against unlawful or unauthorised processing of Personal Data and against accidental loss, or damage to Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

10 Accountability & Governance

10.1 The accountability principle requires the College to demonstrate that it complies with the Personal Data Principles and states explicitly that this a whole College responsibility.

10.2 To demonstrate that the College complies we must:

- implement appropriate technical and organisational measures that ensure and demonstrate compliance. This will include internal data protection policies such as staff training, internal audits of processing activities,
- maintain relevant documentation on processing activities;
- appoint a Data Protection Officer;
- implement measures that meet the principles of Personal Data by Design and Data Protection by Default.
- practice data minimisation and use pseudonymisation when appropriate.
- be transparent in relation to how we use and manage Personal Data;
- allow individuals to monitor our processing of Personal Data;
- create and improve security features on an ongoing basis;
- use Data Protection Impact Assessments (DPIA) where appropriate.

11 Responsibilities of Staff

11.1 Staff means, employees, contractors, agency staff and any other person working for Walsall College.

11.2 This policy does not form part of the formal contract of employment, but it is a condition of employment. Employees will abide by the rules and policies made by the College, which may be updated from time to time.

11.3 Staff must ensure that they understand and adhere to the contents of this Data Protection Policy and associated procedures.

All staff are responsible for:

- Checking that any information that they provide to the College in connection with their employment is accurate and up-to-date.
- Inform the College of any changes to information, which they have provided. i.e. changes of address, or contact details.
- Complying with the staff guidelines for data protection in Appendix 4

11.4 Staff should complete the mandatory staff training on data protection, promptly, when asked to do so. Failure to do so may result in disciplinary action.

11.5 Any member of staff, who considers that the policy has not been followed in respect of Personal Data about themselves or others, should raise the matter with the College's Data Protection Officer.

11.6 All staff are responsible for ensuring that:

10.6.1 Any Personal Data has been collected and processed in a fair and lawful manner.

10.6.2 Personal Data which is held is kept securely whether in paper or electronic format.

10.6.3 Any Personal Data is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

11.6.4 Personal Data that is processed for one reason is not reused for another unrelated reason without seeking consent from the individual.

11.6.5 All Personal Data is treated with a high degree of sensitivity and disposed of using the confidential waste consoles.

11.7 Any breach of data security must be reported immediately to the Data Protection Officer, using the Data Breach Incident form available on the Data Protection SharePoint site. All data breaches will be logged and investigated. The College may need to report the breach to the ICO (dependant on breach) within 72 hours, immediate reporting is essential.

Records Management

Paper Storage

11.8 Paper based records containing Personal Data should be kept in a manner which ensures that they are protected from the risk of a data breach, e.g. unauthorised access / disclosure, accidental loss, Appropriate measures should be used to protect these records such as being in a locked room, filing cabinet, drawer or other appropriate storage device.

Electronic Storage

11.9 The storage or use of any Personal Data processed by the College directly onto the hard disk devices, such as personal computers or personal mobile devices must be avoided unless it is necessary. The recommended mechanism for using such data is to keep the personal data on the College's secured network drives, secure servers in Office 365, Google Apps for Education, SharePoint or College central systems.

Mobile Devices

11.10 Mobile devices include; laptops, tablets, smart phones, mobile phones or other devices capable of storing Personal Data owned by staff or Walsall College.

11.10.1 Mobile devices containing Personal Data owned by the College must use an approved Walsall College method to protect the personal data.

11.11 Approved methods of protection of Personal Data include encryption and the use of other tools as identified and deployed by the DPO or the Head of IT.

11.12 The use of non- approved portable storage devices, including USB sticks / flash drives and unencrypted file sharing mechanisms e.g. Dropbox is prohibited in line with the E-Communications Policy. Approval for use can only be obtained from the ICT Helpdesk.

11.13 Laptops must employ full disk encryption with approved Walsall College encryption software. Personal Data that belongs to Walsall College must not be stored or copied onto a laptop that is in an unencrypted form.

11.14 Smart phones and tablets provided to Walsall College staff for business use will be secured with a PIN code as a minimum standard of protection. The College will also employ remote wipe technology to remotely disable and delete any Personal Data that is stored on the mobile device, which is reported as lost or stolen.

11.15 The use of personal mobile devices for College business must be approved by the IT department and in line with the College's E-communications Policy.

11.16 If you choose to synchronise your College email account to your mobile device, you must protect the device with a pin/passcode and enable device encryption. If you require advice on how to do this, please contact IT Services.

11.16 The loss or theft of any mobile device or portable storage device containing the College's Personal Data must be reported immediately to the Data Protection Officer and the IT helpdesk.

11.17 Deliberate unauthorised disclosure of Personal Data or failure to adequately secure Personal Data either stored on paper or electronically will usually result in a disciplinary matter.

12 Student Responsibilities

12.1 Students must ensure that all Personal Data provided to Walsall College is accurate and up to date to enable the College to comply with the Accuracy principle. They must ensure that changes of address, etc. are notified using the Change/Verify Student Details Form, which is available from Information Services. This will enable the College to update its Management Information Systems.

12.2 Students must ensure that they make use of personal and College equipment in line with the E-Communications Policy and this Data Protection Policy.

13 Data Security Breaches

13.1 All data security breaches must be reported to the Data Protection Officer in line with the Data Breach Plan.

14 The Data Controller and the Data Protection Officer

14.1 Walsall College is:

- The Data Controller for its staff and student information.
- The Education and Skills Funding Agency (ESFA) and the College acknowledge that they are both Data Controllers in common.
- (joint Data Controllers) of the Personal Data collected and held by the College in performing the services and provided to the ESFA.

14.2 The College's designated Data Protection Officer is:

Name: Gurpreet Sandhu
Tel: 01922 657014
Email: gsandhu@walsallcollege.ac.uk

14.3 In the absence of the Data Protection Officer, any issue needing urgent attention relating to the provisions of this policy should be raised with the Deputy Data Protection Officer, Laura Pincher 01922 688658, the Principal, or other member of the Senior Leadership Team acting on behalf of the Data Protection Officer. Depending on the nature of the matter, the data protection team may notify the College's professional indemnity insurer.

14.4 The designated Information Asset Owners at the College are members of the Senior Management Team. Information Asset Owners are responsible for managing, protecting, using and sharing Information Assets within their normal line management responsibility within the college. See the Information Asset Owners job role on our Data Protection SharePoint page.

15 Retention of Data

15.1 The College will keep some forms of information for longer than others. The College's Data Retention Policy provides details of the recommended and statutory periods. Staff must ensure that the retention and destruction of Personal Data is in line with the policy and the Storage Limitation principle

16 Working off College Site

16.1 Staff must ensure that when working off College premises that they adhere to this Data Protection Policy at all times and ensure that their practice is in line with the Home Working Guidance in Appendix 5.

16.2 Staff are responsible for ensuring the security of the College's property and all College information, files, documents, data etc. within their possession, including both paper and electronic material.

17 Conclusion

17.1 Compliance with the GDPR and other data protection legislation is the responsibility of all members of staff and students of the College. Any deliberate or repeated breach of the data protection policy may lead to disciplinary action being taken, or access to the College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated Data Protection Officer.

17.2 Further guidance on Data Protection is available from the following website: https://sharepoint.walsallcollege.ac.uk/sites/departments/data-protection/Pages/Home.aspx

Appendix 1

Data Protection Principles

The General Data Protection Regulation (GDPR) contains six key Data Protection Principles, which set out the main responsibilities for organisations. There is also a seventh 'accountability' principle

The First Principle

Personal Data shall be processed lawfully, fairly and in a transparent manner

The Second Principle

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

The Third Principle

Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

The Fourth Principle

Personal Data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

The Fifth Principle

Personal Data shall be kept in a form, which permits identification of Data
Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

The Sixth Principle

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Accountability Principle

The Data Controller shall be responsible for and be able to demonstrate compliance with the principles.

Appendix 2

Consent Guidance

The GDPR defines consent as:

"Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her."

The General Data Protection Regulations (GDPR) sets a high standard for consent. However, you often will not need consent. If consent is difficult, look for a different lawful basis.

Consent means offering individuals a real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.

The GDPR is clear that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in) and given freely by individuals.

Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent. Walsall College staff should take extra care to show that consent is freely given, and should avoid over-reliance on consent.

Consent is one of the lawful basis for processing, and explicit consent can legitimise the use of special category data. Consent may also be relevant where the individual has exercised their right to restriction, and explicit consent can legitimise automated decision-making and overseas transfers of data.

Relying on inappropriate or invalid consent could destroy trust and harm your reputation – and may leave the College open to large fines.

When is consent appropriate?

Consent is one of the lawful basis for processing, but there are alternatives. Consent is not inherently better or more important than these alternatives. If consent is difficult, you should consider using an alternative. You can check which lawful basis is most appropriate to use by using the interactive Lawful Basis tool, the Information Commissioner's Office.

Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. However, if you cannot offer a genuine choice, consent is not appropriate. If you would still process the Personal Data without consent, asking for consent is misleading and inherently unfair.

If you make consent, a precondition of a service, then it is unlikely to be the most appropriate lawful basis.

Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given.

An imbalance of power occurs in the employment context. Given the dependency that results from the employer/employee relationship, it is unlikely that the Data Subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of

detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent. Therefore, consent is considered problematic for employers to process Personal Data of current or future employees based on consent, as it is unlikely to be freely given. For the majority of such, data processing at work, the lawful basis cannot and should not be the consent of the employees due to the nature of the relationship between employer and employee.

Asking for Consent

In order to ensure compliance with the GDPR you should ensure that:

- You have checked that consent is the most appropriate lawful basis for processing.
- Made the request for consent prominent and separate from other terms and conditions.
- Ask people to positively opt in.
- Do not use pre-ticked boxes or any other type of default consent.
- Do use clear, plain language that is easy to understand.
- Specify why you want the data and what you are going to do with it.
- Give individual ('granular') options to consent separately to different purposes and types of processing.
- Name the College and any third party controllers who will be relying on the consent.
- Tell individuals they can withdraw their consent at any time, and tell them how they can do it.
- Ensure that individuals can refuse to consent without detriment.
- Avoid making consent a precondition of a service.

If you offer online services directly to children, seek consent from children 13 years and over, use age-verification measures (and obtain parental-consent measures for younger children).

Recording consent

The GDPR requires that you keep records of when and how you get consent from the individual. You should also keep a record of exactly what the individuals were consenting to at the time.

Managing consent

To manage consent properly you should regularly review consents to check that the relationship, the processing and the purposes have not changed.

You should have processes in place to refresh consent at appropriate intervals, including any parental consents. There is no set time limit for consent. How long it lasts will depend on the context.

Consider using privacy dashboards or other preference-management tools as a matter of good practice.

You must make it easy for individuals to withdraw their consent at any time, and publicise how to do so and act on withdrawals of consent as soon as possible.

You must not penalise individuals who wish to withdraw consent.

If someone withdraws their consent, this does not affect the lawfulness of the processing up to that point. However, it does mean that the College can no longer rely on consent as its lawful basis for processing. You will need to stop any processing that was based on consent. You are not be able to swap to a different lawful basis for this processing (although you may be able to retain the data for a different purpose under another lawful basis if it is fair to do so – and you should have made this clear from the start). Even if you could originally have relied on a different lawful basis, once you choose to rely on consent you are handing control to the individual. It is inherently unfair to tell people they have a choice, but then continue the processing after they withdraw their consent.

If someone withdraws consent, you should stop the processing as soon as possible. In some cases, it will be possible to stop immediately, particularly in an online-automated environment. However, in other cases you may be able to justify a short delay while you process the withdrawal.

You must include details of the right to withdraw consent in your privacy information and consent requests. It is good practice to include details of how to withdraw consent.

In some cases, you may need to keep a record of the withdrawal of consent for your own purposes – for example, to maintain suppression records so that you can comply with direct marketing rules. You don't need consent for this, as long as you tell individuals that you will keep these records, why you need them, and your lawful basis for this processing (e.g. legal obligation or legitimate interests).

Appendix 3

Withdrawal of Consent Form

I..... (insert full name), Student/Staff ID Number.....

wish to withdraw my consent to the processing of my:

Please tick all that apply

Personal Data that the College has recorded, in the following categories:

a) Personal details including name, address, date of birth etc. ☐

b) Use of photographs for promotional purposes ☐

c) Use of other Personal Data for promotional purposes ☐

Special category data that the College has recorded, in the following categories:

a) Race, religion, ethnic origin ☐

b) Health and medical matters ☐

c) Sexual orientation and sex life ☐

d) Political, religious or trade union membership information ☐

e) Criminal convictions/ offences ☐

Other information.....

.....

.....

Please state which department, you would like to withdraw consent from:

Department:.....

Signature..... Date.....

Please note the College may not require consent for the processing of some data e.g. in order to fulfil its statutory obligations.

Appendix 4

Staff Guidelines for Handling Personal Data

1 Staff will process data about students on a regular basis, when marking registers, or College work, writing reports or references, or as part of a pastoral or academic supervisory role. The College will ensure through registration procedures, that all students understand the lawful basis for this sort of processing, and are notified of the categories of processing, as required by the GDPR. The Personal Data that staff deal with on a day to day basis will be 'standard' and will cover categories such as:

- general personal details such as name and address.
- details about class attendance, coursework marks and grades and associated comments.
- notes of personal supervision, including matters about behaviour and discipline.

2 Information about a student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is Special Category Personal Data and can only be collected and processed with the student's consent. Consent is obtained on the processing of ethnicity data at enrolment. However, if staff members need to record any other information, they should seek the learner's written consent. For example: recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a learner is pregnant, as part of pastoral duties.

3 All staff members have a duty to make sure that they comply with the GDPR principles, which are set out in the Data Protection Policy.

4 Should a member of teaching staff consider it necessary to collect Special Category Personal Data or be asked to process this data, outside of the above setting they should refer to their line manager in the first instance.

5 It is the responsibility of all staff to ensure that all data is kept securely and in line with all the Data Protection Principles.

6 Staff shall not disclose Personal Data to any other staff member, who does not have a legitimate business need to access the data, except with the authorisation or agreement of the designated Data Protection Officer, or in line with the Walsall College policy.

7 Before processing any Personal Data, all staff should consider this checklist.

Staff Checklist for Recording / Processing Data

- Do you really need to record the information?
- Is the information Personal Data or is it Special Category Personal Data?
- If it is Special Category Personal Data, do you have a lawful basis and an appropriate condition to process the data?
- Has the learner been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the Data Subject that the data is accurate?
- Are you sure that the data is secure?

Appendix 5

Home Working Guidance

This guidance applies to all staff who use or access Walsall College systems or information remotely either occasionally or as part of their contract. It applies to information in all formats, including manual records and electronic data.

'Remote working' means working off campus or outside of the secure Walsall College computing environment, this includes working while connected to the Walsall College Wi-Fi networks.

This guidance gives general advice on the issues you need to consider in order to ensure that any information you work on at home or off College premises is protected from loss or unauthorised access and exploitation, whilst also ensuring that the information is accessible to anyone that needs to use it for their work. It applies to information in all formats, including paper files, electronic data, word processed documents and e-mails.

The Data Protection Act 2018 and the Freedom of Information Act 2000 apply to all information that you receive and create as part of your employment regardless of where you work on or store the information.

The primary copy of College information should not be stored at home. Instead College records stored on College networks or systems should be updated as soon as possible with copies of any work that you do at home. This applies to all teaching or administrative work. This allows anyone who needs to refer to the record in your absence, to be able to access the most up-to-date information. It will ensure there is a backup copy of the work, if you were to lose your work at home. Finally, it will enable the College to respond to any Freedom of Information or Data Protection requests for the information, without having to ask you to search for the information you have at home.

You will need to take reasonable measures to protect the information from unauthorised loss, access or amendment whilst stored at home. This will enable the College to comply with our Data Protection obligations and is in the College's business interest (depending on the nature of the information involved), if someone inappropriately gained unauthorised access to the information. It can cause reputational, commercial or competitive damage to the College, for example sensitive information about students or staff.

When using a personal device it is recommended that you use a broadband connection to work directly from/to the appropriate College server via the Home Access link on the College website. College supplied devices will automatically connect to the college network over a secure Direct Access link allowing you to securely access your home drive and shared folders over a broadband connection.

This will remove the need to take home electronic information or to store it there. Using Walsall College supplied devices will mean that when you work at home you will need to take fewer precautions concerning keeping electronic information secure and your principal concern will be to protect your paper information.

The paper information you use at home or when working off site is most vulnerable to loss or unauthorised access in the following ways:

- As a result of leaving papers in areas where they may be seen by others. This is most likely to cause difficulties when the information is about identifiable individuals.
- As a result of crime.
- As result of loss, particularly on the journey to and from work.

All paper information must be held securely within the home environment, e.g. in locked, bags, drawers, filing cabinets, or offices.

Unless you work directly from/to the appropriate College server via Home Access (on the extranet website) the electronic information you work on at home is vulnerable to loss or unauthorised access or amendment in two ways:

1 Physically, through the loss, damage or access to the computer or storage medium on which the record is held, most commonly use of non-approved flash drives or unprotected security access on home computers.

2 Remotely, through someone accessing (hacking) your computer while it is connected to the internet or through a virus.

Anti-virus software is preloaded onto all College equipment. (Always ensure your computer system and applications are up to date with security software – Windows users can use the Windows update site to help with this. Always use a firewall, Windows firewall is sufficient but enhanced protection may be provided by your internet service provider, or be available as part of the router or through installation of a personal firewall package). To ensure Windows Firewall is enabled go to Control Panel and Window Firewall. Similarly, if you are on a Mac you can check the firewall is enabled by going to System Preferences, Security, and Firewall.

When deciding what reasonable security precautions you need to take against these vulnerabilities, it is necessary to balance their financial cost, time and practical implications against the seriousness of the damage that would result if someone did see the information or made unauthorised alterations to it. Depending on the nature of the information, this damage could entail legal proceedings against you or the College, damage to the College's reputation; or damage to collaborative relationships caused by the inappropriate release of information. If you have used your home PC to work on sensitive College information or personal identifiable information when you dispose of the computer you must make arrangements to ensure that the sensitive information is no longer accessible.

You should not store the official primary copy of College information on a laptop that is regularly away from the office; as the information is not readily accessible and is vulnerable to loss or theft. You should ensure that appropriate security measures are taken to prevent unauthorised access to the information. Finally, you should never use a non-College e-mail for College business. All College email accounts are accessible via the internet.

Summary:

1 Ensure all paper records containing Walsall College information are properly protected when taken off site.

2 Try to ensure you use a Walsall College supplied mobile device or laptop to access or store College records to reduce risk.

3 If you do use a personal device or laptop to access College data, connect to the network remotely and do not store copies locally on the device.

If you require further information or support, please contact the Data Protection team.