ASHWICKE HALL SCHOOL
Bath, UK

DATA PROTECTION POLICY

This policy applies to the whole school workforce; those employed to teach or otherwise engaged to work or volunteer at Ashwicke Hall School, including boarding.

This policy is publicly available on the Ashwicke Hall School website and on request; a copy may be obtained from the school office. All who work, volunteer or supply services to our school have an equal responsibility to understand and implement this policy and its procedures, both within and outside of normal school hours and including activities away from school. This policy should be read and understood in conjunction with our Safeguarding – Child Protection Policy, Anti-Bullying Policy, Whistleblowing Policy, Data Retention Policy, Data Breach Policy and The Staff Code of Conduct.

Monitoring and Review: This policy is subject to continuous monitoring, refinement and audit by the Board of Directors, which will also undertake a full annual review of this policy and procedures, inclusive of its implementation and the efficiency with which the related duties have been implemented. This review will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the updated/reviewed policy and it will be made available to them in either hard copy or electronic format.

Signed:

Reviewed: March 2019
Next Review Date: March 2020

Ms Amanda Woods
Principal

This policy was last reviewed by the Executive Regional Director and the Principal in March 2019 and will next be reviewed in March 2020 or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

If you want to see a copy of information about you that we hold, please contact David Dunce, Accountant, Ashwicke Hall School, Ashwicke Hall, Marshfield, Nr Chippenham, Wilts. SN14 8AH. Tel: 01225 891841.

Introduction

This Data Protection Policy ("Policy") regulates and details the way in which Ashwicke Hall School ("the School") obtain, use, hold, transfer and process Personal Data and Sensitive Personal Data (as defined in parts 2 and 7 of this policy) about individuals and ensures that all School employees know the rules for protecting Personal Data.

This Policy also describes individuals' rights in relation to their Personal Data processed by the School.

The School has practices in place in relation to their handling of Personal Data to ensure that they are acting in accordance with UK laws and other relevant regulatory guidance. The most notable legislation in this area is the Data Protection Act 1998 (DPA), The Privacy and Electronic Communications (EC Directive) Regulations 2003 (last updated 2016) (PECR) and the General Data Protection Regulations (GDPR) enacted in 2018.

The School shall comply with the principles of the DPA to ensure that all data is:

- accurate and kept up-to-date;
- collected fairly and for lawful purposes only;

- processed by the company within its legal and moral boundaries; and
- protected against any unauthorised or illegal access by internal or external parties.

Our data will not be:

- communicated informally;
- stored for more than a specified amount of time;
- transferred to organisations, states or countries that do not have adequate data protection policies; or
- distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities).

In addition, the School will also comply with the GDPR that introduces further rights for individuals and strengthens some of the rights already in existence under the DPA including the right to:

- let people know which of their data is collected;
- inform people about how we'll process their data;
- inform people about who has access to their information;
- have provisions in cases of lost, corrupted or compromised data; and
- allow people to request that we modify, erase, reduce or correct data contained in our databases.

At all times, the School will endeavour to ensure that it has a legal basis for the processing of personal information. Ashwicke Hall School is registered as a Data Controller with the Information Commissioner's Office (ICO). The School's Accountant acts as the Data Protection Officer and is available to contact on any Data Protection issue.

Personal Data

"Personal Data" is any information (for example, a person's name) or combination of information about a living person (such as name and address and date of birth) which allows that living person to be identified from that information and which relates to them, such as the job application of "Joe Green" with his address and date of birth, or the academic record of "Sam Brown" with similar details. If in doubt, individual details should be treated as Personal Data.

Examples of Personal Data which may be used by the School in its day to day business include employee, student, parent and customer details, such as names, addresses, telephone numbers and other contact details, such as email addresses and mobile numbers, CVs, performance reviews, photos, payroll and salary information. This could affect job applicants, direct employees, temporary staff, volunteers, parents, students, individual consultants or contractors, visitors etc.

Personal Data may also be relevant to unincorporated suppliers or customers or (such as a sole trader business or partnership), or inquirers or complainants, and to individual contacts at third parties, customers and leads, even in respect of work contact details, such as their direct line or mobile number, or information entered about them in any management system.

The definition of Personal Data also includes opinions about a person, and appraisals about or statements of intent regarding them.

The laws governing how the School can use Personal Data apply whether the Personal Data is stored electronically (for example, in emails, on IT systems, as part of a database or in a word-processed document) or in structured paper records (for example, in paper files, card indexes or filing cabinets).

Processing of Personal Data & Audits

The School uses or processes Personal Data (including Sensitive Personal Data) on a range of individuals for a multitude of business purposes. Such individuals may include staff and contractors, students and parents, alumni, business contacts, customers and prospects, job applicants and former employees, and the person whose Personal Data is used by the School is known as "the data subject".

When the School collects, stores, uses, discloses, updates or deletes or destroys Personal Data, this is called "processing". All processing is regulated by data protection legislation and must meet certain conditions to be carried out lawfully. The School maintains a database of personal data held in different School departments, has clear retention schedules and the Data Protection Officer conducts regular audits of Personal Data held. Personal Data and Sensitive Personal Data are held securely by the School and staff are regularly briefed by the ICT department and via the ICT policies on appropriate and safe data management.

The Data Protection Act 1998: How we use information for employees

We process personal data relating to those we employ to work at, or otherwise engage to work or volunteer at, our school. This is for employment purposes to assist in the running of the school and/or to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector;
- enabling development of a comprehensive picture of the workforce and how it is deployed;
- informing the development of recruitment and retention policies;
- allowing better financial modelling and planning;
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body.

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- our local authority;
- the Department for Education (DfE).
- Pension providers
- HMRC

If you require more information about how we and/or DfE store and use your personal data please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Legislation and Information Commissioner's Office

Data protection laws are enforced in most countries by the local Data Protection Authority: in the UK, this is the Information Commissioner's Office (the "ICO"). The ICO may investigate concerns and complaints, may audit the School's use or processing of Personal Data, and may take action against the School (and in some cases individuals) for breach of these laws. Action may include making the School pay a fine and/or stopping the use by the School of the Personal Data, which may prevent it from carrying on its business. There is also the risk of negative publicity. In addition, the General Data Protection Regulations (GDPR) 2018 update current legislation and will be directly applicable in all EU Member States (and those wishing to engage and trade with those states) without the need for implementing national legislation. This introduces more stringent data protection obligations on Data Controllers and was initiated by UK Government.

Transparency and Personal Data

The School is entrusted to use the Personal Data of individuals on the basis that the proposed use is transparent, expected and clearly defined. Accordingly, one of the main data protection obligations requires the School to process Personal Data fairly. In addition, use of Personal Data must be lawful. In practice, this means that the School will comply with at least one of the following conditions when processing Personal Data:

- the individual to whom the Personal Data relates has consented to the processing;
- the processing is necessary for the performance of a contract between the School and the individual (or to enter into that contract at the individual's request);
- the processing is necessary to comply with a legal obligation (not a contractual obligation) placed on the School;
- the processing is necessary to protect a vital interest of the individual (where there is an imminent risk to their life or of serious harm to them otherwise); or

- the processing is necessary to pursue the legitimate interest of the School (or a proposed recipient of the Personal Data) but where on balance, this would not involve disproportionate harm to the individual.

Use of Personal Data should meet one or more of these conditions. If it is proposed that Personal Data should be used for a purpose different to that for which it was originally collected, the above conditions must be considered, and the Data Protection Officer consulted. All new Personal Data processing activities and projects involving the use of Personal Data must be approved prior to being started as there are complex exemptions and other lawful reasons for processing which may apply. For example, if someone provides their details as a contact, you will not be able to start sending them marketing emails unless that is covered in an appropriate notice and consent from that individual.

In addition, the School ensures its Personal Data is accurate and up to date (except where it is stored specifically for historical or archival purposes). The School takes care to record and input Personal Data accurately. Some Personal Data may change from time to time (such as addresses and contact details, bank accounts and the place of employment). Ashwicke Hall School expects staff, volunteers, contractors and parents/guardians of students to inform us of changes in personal detail but will make all reasonable efforts to ensure reminders are issued. The School takes care to update records promptly and correctly when notified of changes.

Privacy Notices

When an individual gives the School any Personal Data about him or herself, or a parent/guardian provides details on behalf of a child, the School will make sure the individual knows:

- who is responsible for the Processing of their Personal Data;
- for what purposes that School will process the Personal Data provided to it;
- sufficient details about any proposed disclosures/transfers of their Personal Data to Third Parties (including any cross-border transfers);
- the rights that the individual has in respect of their personal data;
- any other information that the individual should receive to ensure the processing carried out is within his/her reasonable expectations (retention periods for instance); and
- who to contact to discuss or raise any Personal Data issue.

The School does this by providing this information is known as providing a "privacy notice" or fair processing notice. Before collecting Personal Data, staff at the School will give individuals providing those details appropriate Privacy Notices; these may be embedded in contracts, or on websites or form part of application or other forms. The School will inform individuals about the processing of their Personal Data before or at the time the data is collected. The information contained in its Privacy Notices will be concise and easily accessible and written in clear and plain language. The School will only process Personal Data in a manner and for purposes consistent with the relevant privacy notice(s) already provided to an individual. Personal Data should not be collected for one purpose and then used for a second purpose unless that is also set out in the relevant notice.

Sensitive Personal Data

"Sensitive Personal Data" is Personal Data about a person's race or ethnicity, their health, their sexual preference, the medical information, their religious beliefs, their political views, trade union membership or information accusing an individual of any crime, or about any criminal prosecution against them, and the decision of the court and any punishment. The Data Protection Officer can provide further information on what is, and the handling of, Sensitive Personal Data. Sensitive Personal Data should not be collected or used unless essential. It must be treated as strictly confidential.

Extra care must be taken with it and it must be kept more securely. In addition to the normal requirements for lawful use of any Personal Data such details should not be used without the explicit prior consent of the individual, which has to be clear, unambiguous and voluntary. The School does not seek to obtain Sensitive Personal Data unless:

- the individual concerned agrees in writing that we may do so, on the basis of a full understanding of why the School is collecting the data;

- the School needs to do so to meet its obligations or exercise its rights under any relevant laws; or
- in exceptional circumstances such as where the processing is necessary to protect the vital interests of the individual concerned.

Please note that the "legitimate interest" criteria described above alone is not enough to process Sensitive Personal Data. Sensitive Personal Data should not be disclosed unless measures are taken to encrypt or otherwise secure that information due to the potential for harm or distress if the email is received by unintended recipients or otherwise goes astray. Sensitive Personal Data should be collected and used as little as possible and be subject to more limited and strictly need to know access and used subject to greater security measures than other Personal Data. Other Personal Data where misuse may lead to distress or harm, especially to fraud or identity theft (for example, bank account or credit card details, or official government identification numbers, such as national insurance contribution numbers) or DBS and barring list checks must be treated like Sensitive Personal Data.

Employee Obligations

All School staff should be aware of their obligations and comply at all times with this Policy. All staff must ensure that Personal Data collected by them must be appropriate to and sufficient for the relevant purpose(s) for which it is collected but not excessive for that purpose(s). Use of Personal Data should be minimised and not maximised. Collecting unnecessary personal Data adds to the School's compliance burden. Where staff are dealing with student and parent data already collected by the School, (on SSMS for example) the individual/s concerned will have given consent on joining the School for the processing of their personal data for the purposes of running the School. All staff involved in the processing of personal information will:

- read and understand this policy;
- use strong passwords and two-step authentication;
- encrypt all portable devices if they contain personal data; and
- only keep information as long as necessary.

Staff should not download personal data on to personally owned devices unless absolutely necessary. In such cases, the personal data should be deleted from the personal device as soon as is practicable after use.
Please see Appendix 1 for further guidance.

Data Retention & School Archives

Please refer to the Ashwicke Hall School Data Retention Policy for guidance and retention periods.
Personal Data must be stored securely and not be kept for any longer than required. Some records have to be retained for minimum periods by law (such as records on employee payments and their taxation under tax laws). As a general rule, when Personal Data is no longer needed for the purposes for which it was collected, this Personal Data will be securely and permanently destroyed as soon as practicable. The School will not delete or destroy or amend records containing Personal Data without explicit consent once they have been informed those records have been requested by the individual whose Personal Data it is, or by a Data Protection Authority. Such a breach may be a criminal offence with personal liability.

Some data that is used for research purposes (and that is compatible with the purposes for which the data was originally collected) may be kept indefinitely if the relevant conditions apply. These are: that the data is not processed to support decisions about individuals, and that substantial damage or substantial distress is not likely to be caused to any data subject. Personal data can be selected for permanent preservation, and stored, if these two conditions apply, on condition that the other data protection principles are complied with. It is expected that historical data being preserved for the School archives should normally be anonymised.

The Right to Information, the Right to Erasure and Subject Access Requests

Individuals have certain rights in relation to their Personal Data. These include:

- the right to obtain information (what Personal Data, from where, used for what purposes and shared with which recipients) about Personal Data held about themselves and to obtain copies of such Personal Data (Subject Access Request);
- the right to prevent processing of Personal Data for direct marketing purposes;

- the right to object to and stop certain processing of Personal Data where it is likely to cause substantial unwarranted harm or distress;
- the right to have Personal Data corrected;
- the right to compensation for any damage/distress suffered from any breach;
- the right to be informed of automated decision making about them.

If any member of School staff receives such a request or demand from an individual, they must promptly inform the Data Protection Officer. Individuals are also allowed to withdraw their consent to the School's use of their Personal Data at any time. If a School employee receives such a withdrawal of consent, they must promptly inform the Data Protection Officer. If anyone at the School receives a request to stop sending marketing materials, direct marketing communications of that type to that individual must be stopped as soon as is possible. Individuals can also ask in writing for copies of their Personal Data which the School holds about them and other details about how the School uses their Personal Data.

Subject to receipt of proof of ID (and payment of any official fee permitted which the School has requested), following receipt of a written request from an individual for access to his/her Personal Data, the School will (to the extent requested by the individual):

- inform that individual whether the School holds Personal Data about him or her;
- describe the Personal Data about the individual which it holds, the reason for holding the Personal Data and the categories of persons to whom it may disclose the Personal Data; and
- provide the individual with copies of the Personal Data held about him or her, together with an indication of the source(s) of the Personal Data.

Strict rules must be followed as part of this process. Therefore, any such request received should be passed on to the Data Protection Officer. There are strict statutory deadlines for responding. School staff must not respond to any such request directly. There is a right under the DPA known as "the right to be forgotten". This gives individual the right to have their data erased when there is no compelling reason for continued processing. Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this test is not present. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

Please note, a Data Subject does not have the right to see Personal Data about other individuals, even if related to their own circumstance. It is therefore Ashwicke Hall School's policy to redact documents or copies before sharing them with a Data Subject, where appropriate, to protect the privacy of others.

Data Security

Please see Appendix 1 of this Policy for guidance on remote access and working.

The School endeavours to keep all Personal Data secure by protecting it from being accessed by other companies or individuals (for example, via hacking), from being corrupted (data corruption) or being lost or stolen. This applies to Personal Data whether held electronically or in paper files. For example, School staff [and School Contractors and volunteers where relevant] each have a password and individual controlled access rights to IT systems through their School computer and/or mobile or another electronic device. For further information, please refer to the School's ICT policies.

School staff must comply with the School's security procedures whenever processing Personal Data. The School is dependent upon all employees to help keep Personal Data secure. Employees must only access and use Personal Data they are individually authorised to access and use, and which is needed for a specific task within their School role.

The School also recognises that adequate security is important where it arranges for Third Parties to process Personal Data on its behalf, such as when outsourcing services to service providers, who process Personal Data on behalf of the School as a result ("a Data Processor"). The School remains liable for those service providers and their

treatment of the Personal Data. The School will have suitable written contracts in place with such service providers with specific terms included to protect the Personal Data provided to them.

Disclosing Personal Data to Third Parties and Overseas Transfers

A disclosure of Personal Data is a form of processing. That means that the rules described above for fair and lawful use have to be satisfied. The School will not disclose Personal Data to a Third Party without first checking the disclosure is lawful and proportionate. There are some exceptions to deal with disclosures, such as those requested lawfully by police where the information is necessary to prevent or detect a crime. Any request for Personal Data about an individual from government, police or other similar bodies or from journalists or other investigators should be passed immediately to the Data Protection Officer.

From time to time the School may pass student personal data (including sensitive personal data where appropriate) to third parties where lawful to do so, including local authorities, other public authorities, such as Ofsted, health professionals, and the School's professional advisers, who will process the data:

- to enable the relevant authorities to monitor the School's performance;
- to compile statistical information (normally used on an anonymous basis);
- to secure funding for the School (and where relevant, on behalf of individual students);
- to safeguard students' welfare and provide appropriate pastoral (and where relevant, medical and dental) care for students;
- where specifically requested by students and/or their parents or guardians about themselves;
- where necessary in connection with learning and extra-curricular activities undertaken by students;
- to enable students to take part in national and other assessments and to monitor students' progress and educational needs;
- to obtain appropriate professional advice and insurance for the School;
- where a reference or other information about a student or ex-student is requested by another educational Ashwicke Hall School is committed to safeguarding and promoting the welfare of students and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential. Page 8 of 8 establishment or employer to whom they have applied; or
- otherwise where reasonably necessary for the operation of the School.

Unlawful disclosure (however well-meaning and however seemingly authoritative the requestor) risks placing the School in breach of several obligations under data protection legislation. Special care is needed with telephone requests for information, often used by unauthorised parties to ‘blag’ or obtain Personal Data to which they are not entitled. School employees must be certain of the identity of the person with whom they are dealing, ideally have a written request for information from them and ensure any disclosures are justified and authorised in advance. Please see our Data Breach Policy for guidance on what to do in case of a breach.

There are special rules on whether Personal Data can be transferred to another country. Within the EU, there are restrictions on the transfer of Personal Data outside of the European Economic Area (EEA) (such a transfer is considered to be, for example, where Personal Data is emailed outside the EEA; where the School IT servers are hosted outside the EEA; or where there is remote on-screen access from outside the EEA to Personal Data stored in an IT system within the EEA). This is to make sure the Personal Data remains safeguarded and that the individuals concerned do not lose the protection and rights they have under local law in respect of their Personal Data when transferred. Actual or likely transfers of Personal Data to outside the EEA, especially of Sensitive Personal Data, should be clearly set out in the privacy notices described in the fair use section of this Policy so that such transfers are expected by the affected individuals.

Alumni, Marketing and Fundraising

As with other types of Processing, the use of Personal Data for marketing and fundraising purposes must satisfy the fair and lawful use requirements set out above. This means information notices must be given, and a lawful reason for processing has to be satisfied; typically, this will ~~have to~~ be consent based. Personal Data should not be used to contact individuals for marketing purposes by email, text or similar unless the individual has consented to marketing use. Individuals have a right to decline postal marketing and to object to any fundraising. Where marketing or

fundraising is to be by phone, email, text or similar electronic means, individual consent is needed and must clearly cover marketing by that communication method. Special rules apply as to when consent is needed and how consent is obtained (for example, marketing activities must now be "opt in" and not "opt out" depending on the type of marketing contemplated and the means of communication with the individual. Any objections to marketing or requests to unsubscribe must be dealt with. School employees should liaise with the Data Protection Officer about any marketing or fundraising plans regarding compliance with regulation on Data Protection.

Please note, in addition to DPA and GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (amended 2016) apply to electronic marketing activities such as 'phone and email marketing, the use of cookies on websites and the compilation of directories.

Appendix 1: Data Security – remote access and work from home

This policy applies to all staff or volunteers logging in remotely to Ashwicke Hall School servers or taking work home with them; it applies to School-supplied equipment and to individual's own equipment or networks when being used for Ashwicke Hall School business.

Ashwicke Hall School recognises that, sometimes, it is convenient for staff to take work home with them or to log in remotely to complete tasks. In all cases, staff are reminded that they are responsible for the security of all data, whether held electronically or physically, and must ensure it is stored securely to maintain confidentiality of information from members of the family or visitors. Staff are reminded that a data breach occurring in this way may result in the instigation of the Schools disciplinary procedures.

Further information on data protection is held within the School's Data Protection Policy. Please see also our Staff Code of Conduct for advice on confidentiality, social networks and portable devices, such as mobile 'phones and personal cameras.

School-owned equipment used outside of School

It is the staff member's responsibility to ensure that the following points are adhered to at all times:

- staff must take due care and attention of portable computer devices when moving between home and school;
- laptops or other portable equipment must never be left unattended in cars or taken into vulnerable areas;
- staff will not install or update any software onto a School owned portable computer device without express permission;
- staff will not install any screen savers onto a School owned portable computer device;
- staff will connect with a wired connection wherever possible. Where a wired connection is not possible, and a wireless connection is used, this should be a secure connection. Personal or sensitive data should not be accessed via wireless connection.
- staff will not install any hardware to or inside any School owned portable computer device, unless authorised by the School's IT Services;
- staff will allow the installation and maintenance of the School's installed Anti-Virus updates immediately;
- staff will inform the IT Services Helpdesk of any School owned portable computer device message relating to configuration changes;
- business critical data should be stored on a School network drive and not held on the portable computer device;
- all faults must be reported to the IT Services Helpdesk;
- staff requests for upgrades of hardware or software must be approved by their Line Manager with financial authorisation. Equipment and software will then be purchased and installed by IT Services;
- no family members may use any School provided equipment. The School provided equipment is supplied for the staff members' sole use;
- staff must ensure that reasonable care is taken of the School equipment supplied. Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. It is recommended that the office area of the house should be kept separate from the rest of the house. Equipment must be secured whenever it is not in use by either locking away in a cupboard or drawer or by locking the device to the desk (suitable locks can be provided by IT Services);

- staff should seek advice from the School before taking any School supplied equipment outside the United Kingdom. The equipment may not be covered by the School's normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel;
- the School may at any time, and without notice, request a software and hardware audit and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.

Personal equipment used for School business

Staff who chooses to undertake work at home or remotely in relation to their official duties using their own IT equipment must understand that they are not permitted to hold any database or carry out any processing of personal or sensitive information relating to the School, its employees or pupils. Under no circumstances should personal or sensitive information be emailed to a private non-School email address. For further information, please refer to the School's Staff Code of Conduct.

Staff accessing the School's servers, or using personal or sensitive information, must only use equipment which has appropriate technical security and advanced authentication mechanisms whilst working remotely. Connection for this device must be with a wired connection and no wireless connections must be used.

Staff are responsible for ensuring that their general software and specific anti-virus software is kept up-to-date in order to avoid inadvertently sharing malware that could infect School's networks and to avoid being the weakest link for hackers to attack School systems. If in any doubt, please consult the School IT Service.

Staff's personal equipment should be password protected.

Access Controls (on all equipment)

It is essential that access to all personal or sensitive information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password or user login controls.

Computers and portable devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes. All data must, where possible, be encrypted. If this is not possible, then all personal or sensitive data held on the portable device must be encrypted. A sufficiently secure remote access mechanism must be configured to allow remote users access to School systems if connecting over Public Networks, such as the Internet.

Two separate means of authentication (i.e. username/password and PinSafe PIN Number or Microsoft Two factor authentication app) must be used when accessing the School network and information systems (including Outlook Web Access / Office 365) remotely via both School owned and non-School owned equipment. Access to the Internet from School owned IT equipment should only be allowed via an onward connection (i.e. you must connect to the School's network first then access the Internet, in order to be protected by the School's security systems).

As compliance criteria on the School become more complex, the IT Service may need to apply further security controls from time to time. Any such changes will be communicated to all staff with access to a School computer. Such security controls may be applicable to School owned and privately-owned devices, should the user not wish their privately-owned device to be subject to security controls then that device may not be allowed to connect to the School network or access School information.

Staff must ensure that access/authentication tokens and personal identification numbers are kept in a separate location to the portable computer device at all times. Removable media devices and paper documentation must not be stored with the portable computer device. Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (eg secure filing cabinets) when not in use. Documents should be collected from printers as soon as they are produced and not left where they can be casually read. Waste paper containing personal or sensitive information must be shredded to required standards (DIN Level 4, Cross cut [1.9mm x 14mm]).

Sensitive material or personal data must be disposed of by recognised methods using office based shredding equipment or other means.