


## **Data Protection Policy**

<b>Classification:</b>	Public
<b>Owner:</b>	Data Protection Officer
<b>Version:</b>	2
<b>Status:</b>	Approved
<b>Governor Committee:</b>	Finance and Premises Committee
<b>Date of approval:</b>	7 March 2022



## **Contents:**

	Page:
<b>Policy Introduction and Purpose</b>	3
<b>Policy Aims</b>	4
<b>Policy Scope</b>	5
<b>Consultation</b>	6
<b>Sources and references</b>	7
<b>Policy/Controls</b>	8
<b>Policy Review and Development</b>	19
<b>Document Version Control</b>	20
<b>Appendices</b>	21

## **Policy Introduction and Purpose**

The purpose of this policy and procedure is to ensure compliance of Hall Cross Academy with all of its obligations as set out in the General Data Protection Regulation (GDPR) 2018 and Freedom of Information legislation.

Hall Cross Academy collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the Academy in order to provide education and associated functions. The Academy may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with GDPR and other related legislation.

The GDPR applies to all computerised data and manual files, if falling within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that is searchable on the basis of specific criteria (to use something like the individual's name to find their information). If this is the case, it does not matter whether the information is located in a different physical location.

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation and shall be reviewed every two years.

## Policy Aims

Hall Cross holds information in many forms including pupil, partner, parent/carer and colleague data. They are trusting us to keep it safe and it is our collective responsibility to protect this information.

Loss of personal information would harm the Academy, our pupils, partners and colleagues who are affected. Hall Cross's business could be disrupted, or the brand could be significantly damaged.

Hall Cross Academy recognises that in order that it can operate and meet its legal obligations it needs to collect and use personal data as defined by the Data Protection Act (DPA) 2018 and GDPR. It also recognises that this personal information must be handled appropriately however it is collected, recorded, used or shared with other parties; whether on paper, electronically, or recorded on other material. There are safeguards to ensure this is in accordance with the DPA 2018 and GDPR.

Hall Cross Academy regards the lawful and correct treatment of personal information as very important to its successful operation, and recognises the need to maintain confidence between those with whom it deals and the Academy. As such, Hall Cross actively encourages and requires compliance with the DPA 2018 and the EU GDPR 2018.

## **Policy Scope**

This policy applies to all Hall Cross Academy employees, Governors, contractual third parties and partner organisation employees who have access to any data held or provided to/by the Academy. This includes permanent and temporary staff, consultants, contractors and partner companies.

Information Security is not just a management responsibility, it's everyone's responsibility.

## Consultation

The following groups were involved in developing this policy:

- Staff
- Governors
- External consultants/advisors

## Sources and References

The General Data Protection Regulation 2018  
The Freedom of Information Act 2000  
The Environmental Information Regulations 1992  
The Human Rights Act 1998  
The Regulation of Investigatory Powers Act  
Copyright and Intellectual Property rights  
The Computer Misuse Act  
The Data Protection Act 2018

## Policy/Controls

### Data Controller

The Academy is the Data Controller as defined in the Data Protection Act 2018.

### Notification with the Information Commissioner's Office (ICO)

The Academy notified the ICO, when it was established.

The Academy will renew the registration annually. In addition, if the Academy introduces new purposes for processing information, such as the installation of CCTV, then it will notify the ICO, by email at [notification@ico.gsi.gov.uk](mailto:notification@ico.gsi.gov.uk), requesting that the new purpose be included in the registration.

### Definitions

Personal data is information that relates to an identifiable living individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain. A subset of personal data is known as 'special category personal data'. This special category data is information that relates to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health
- An individual's sex life or sexual orientation
- Generic or biometric data for the purpose of uniquely identifying a natural person

Special Category information is given special protection and additional safeguards apply if this information is to be collected and used.

Information relating to criminal convictions shall only be held and processed where there is a legal authority to do so.

The Academy does not intend to seek or hold sensitive personal data about staff or pupils except where the Academy has been notified of the information, or it comes to the Academy's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with the legal obligation or as a matter of good practice. Staff or pupils are under no obligation to disclose to the Academy their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and/or parenthood are needed for other purposes, e.g. pension entitlements).



## **Data Protection Principals**

The principles of DPA and GDPR require that personal information:

- shall be processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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;
- shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- shall be accurate and, where necessary, kept up to date;
- 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 is processed;
- 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; and
- shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Therefore, Hall Cross Academy will, through appropriate management, procedural and technical controls:

- Ensure that data is only processed lawfully.
- Only retain data for the time period as documented in the Data Retention Spreadsheet.
- Maintain and update the Data Retention Spreadsheet ensuring all new data elements are added as required and existing information is updated.
- The data owner, as identified in the Data Retention Spreadsheet, is responsible for ensuring timely deletion of data in line with stated timelines in the Data Retention Spreadsheet.

## **Conditions for Processing in the First Data Protection Principle**

The Academy holds personal data on students, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined above and there must be a lawful basis for the processing of personal data.

## **Pupils Privacy Notice**

The personal data held regarding students includes contact details, assessment/examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

The data is used in order to support the education of the students, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the Academy as a whole is doing, together with any other uses normally associated with this provision in an Academy environment.

In particular, the Academy may (but is not exhaustive):

- Transfer information to any provider, society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotion purpose in relation to the Academy but only where consent has been obtained in the first instance;
- Make personal information, including sensitive personal information, available to staff for planning curricular or extra-curricular activities; and
- Use photographs of pupils in accordance with parental consent.

Any wish to limit or object to any use of personal data should be made via a request to the Data Controller. If in the view of the Academy Principal, the objection cannot be maintained, the individual will be given reasons in writing outlining why the Academy cannot comply with their request.

## **Employees, Consultants and Volunteers Privacy Notice**

The personal data held about staff will include contact details, employment history, bank details, national insurance number, career progression, DBS check documents and certificates, photographs, special categories including information such as gender, age and ethnic group. The Academy may pass information to other regulatory authorities where appropriate and may use names and photographs of staff in publicity and promotional flyers.

Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as “spent” once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

Any wish to limit or object to the use to which personal information is to be used should be notified to the Data Protection Officer who will ensure that this is recorded, and adhered to if appropriate. If the Data Protection Officer is of the view that it is not appropriate, the individual will be given written reasons why the Academy cannot comply with their request.

The Academy may hold personal information in relation to volunteers, supply staff and governors/directors. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than is necessary.

## **Disclosure of Personal Information to Third Parties**

The following list includes the most usual reasons that the Academy will authorise disclosure of personal data to a third party:

- To give a confidential reference relating to a current or former employee, volunteer or student;
- For the prevention or detection of crime;
- For the assessment of any tax or duty;
- Where it is necessary to exercise a right or obligation conferred or imposed by law upon the Academy (other than an obligation imposed by contract);
- For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

- For the purpose of obtaining legal advice;
- For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
- To disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of Academy trips;
- To provide information to another educational establishment to which a pupil is transferring;
- To provide information to the Examination Authority as part of the examination process; and
- To provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

The Academy may receive requests from third parties (i.e. those other than the data subject, the Academy, and employees of the Academy) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the Academy.

All requests for the disclosure of personal data must be sent to the Data Protection Officer, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

## **Why we Collect Information**

Data collected by the Academy will be in line with GDPR, the DPA and will only be information required to be collected by the Academy to carry out its function and purpose. As such, the Academy will:

- ensure the quality of information used; and
- ensure that the rights of natural citizens, about whom information is held, can be fully exercised including;
  - Right to be Informed
  - Right of Access by the Data Subject
  - Right to Rectification
  - Right to Erasure
  - Right to Restrict Processing
  - Right to Data Portability
  - Right to Object
  - Rights in relation to Automated Decision Making.

The Academy collects information about our pupils, employees and other individuals and holds this personal data so that we can:

- Support each pupil's learning;
- Monitor and report on each pupil's progress;
- Provide appropriate pastoral care and other support to each of our pupils;
- Assess how well each pupil is doing and report on that to the parents;
- Employment purposes;
- To enable the development of a comprehensive picture of the workforce and how it is deployed;
- To inform the development of recruitment and retention policies;
- To assist in the running of the Academy; and
- To enable individuals to be paid.

### **Do we Share this Information with Anyone Else?**

We do not share any of this data with any other organisation without permission except where the law requires it. We are required to provide pupil and staff data to central government through the Department for Education (DfE) [www.education.gov.uk](http://www.education.gov.uk) and the Education Funding Agency (EFA) [www.education.gov.uk/efa](http://www.education.gov.uk/efa).

Where it is necessary to protect a child, the Academy will also share data with the Local Authority Children's Social Services and/or the Police.

### **Can we see the Personal Data that you Hold about our Child?**

All pupils have a right to have a copy of the personal information held about them. Where the child is below the age of 16 years, a request for a copy of the personal information has to be made by a parent or guardian in writing. Data Subject Access Requests are handled centrally and should be referred to the Data Protection Officer (via email - [dpo@hallcrossacademy.co.uk](mailto:dpo@hallcrossacademy.co.uk)).

The only circumstances under which the information would be withheld would be if there was a child protection risk, specifically:

- The information might cause serious harm to the physical or mental health of the pupil or another individual;
- Where disclosure would reveal a child is at risk of abuse;
- Information contained in adoption or parental order records;
- Information given to a court in proceedings under the Magistrate's Courts (Children and Young Persons) Rules 1992; and
- Copies of examination scripts.

To protect each child's right of confidentiality under law the Academy reserves the right to check the identity of a person making a request for information on a child's behalf. Once any identity check has been completed, the information will be collected and provided within 30 calendar days.

## Information Security

### Objective

The information security objective is to ensure that the Academy's information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

### General Security

To protect collected data, the Academy will ensure:

- there is someone with specific responsibility for data protection in the organisation;
- there is a Senior Information Risk Owner in the organisation;
- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- everyone managing and handling personal information is appropriately trained to do so;
- methods of handling personal information are clearly understood;
- methods of handling personal information are regularly assessed and evaluated;
- take appropriate technical and organisational security measures to safeguard personal information. These controls will:
  - Be made in conjunction between the data owner and the GDPR Team
  - Be fully documented on the Data Retention Spreadsheet
  - Be reviewed regularly and/or following major system changes
  - Be in line with all other policies issued by the Academy
  - Follow any vendor issued or industry issued best practice
- that personal information is not transferred abroad without suitable safeguards;
- access to data shall only be provided in line with the Disclosure of Personal Information to Third Parties section of this policy; and
- subject access requests about the storage and handling of personal information are promptly and courteously dealt with.

It is important that unauthorised people are not permitted access to Academy information and that we protect against theft of both equipment and information. This means that we must pay attention to protecting our buildings against unauthorised access. Staff must:

- Be aware of people tailgating you into the building or through a security door;
- Challenge someone they don't know and is not wearing some form of identification;
- Not position monitors/screens on reception desks where members of the public could see them;
- Lock secure areas when you are not in the office;
- Not let anyone remove equipment or records unless you are certain who they are;
- Ensure visitors and contractors in Academy buildings always sign in and records must be kept out of view of visitors to the buildings.

### Security of Paper Records

Paper documents should always be filed with care in the correct files and placed in the correct place in the storage facility.

Records that contain personal data, particularly if the information is sensitive should be locked away when not in use and should not be left open or on desks overnight or when you are not in the office.

Always keep track of files and who has them.

Do not leave files out where others may find them.

Where a file contains confidential or sensitive information, do not give it to someone else to look after.

### **Security of Electronic Data**

Most of our data and information is collected, processed, stored, analysed and reported electronically. It is essential that our systems, hardware, software and data files are kept secure from damage and unauthorised access. Network security is enhanced by the segregation of data, using VLANs. Academy staff must:

- Prevent access to unauthorised people and to those who don't know how to use an item of software properly. It could result in loss of information.
- Adhere to software licensing. Licenses usually only cover a certain number of machines. Make sure that you do not exceed this number, as you will be breaking the terms of the contract.
- Ensure that database access is appropriate to each staff member's role and responsibility, particularly those containing personal data.
- Be aware that data cannot be stored on desktops or local computer document folders. All information should be stored on Google Drive. Personal Data must not be stored in 'my document' folders.
- Not use USB memory devices in school.
- Only connect personal devices to a guest network, allowing access to the internet.

### **User Accounts**

All user accounts are created and deleted centrally by the IT Team, at the request of:

- Staff - HR Officer
- ITT students - Associate Assistant Principal responsible for DRAFTTs
- Students - Data Team

All users are required to adhere to the Acceptable Use Policy.

The disabling of accounts for all parties is carried out on their last day within the Academy. In exceptional circumstances this may be extended.

### **Password Complexity**

- Contain characters from three of the following four categories:
  - Uppercase characters (A through Z)
  - Lowercase characters (a through z)
  - Numeric (0 through 9)
  - Special characters (e.g. !, \$, #, %)
- Minimum password length - 8

Passwords for all applications must be unique.

Passwords for supply staff accounts are changed on a weekly basis.

### **Use of E-Mail and Internet**

The use of the Academy's e-mail system and wider internet use is for the professional work of the Academy. Reasonable personal use of the system in a member of staff's own time is permitted but professional standards of conduct and compliance with the Academy's wider policies are a requirement whenever the e-mail or internet system is being used.

In addition to the demands of the Acceptable Use Policy colleagues must not send:

- Highly confidential or sensitive personal information externally via e-mail, unless it's encrypted.
- Information by e-mail, which breaches GDPR. Do not write anything in an e-mail which could be considered inaccurate or offensive, and cannot be substantiated.

Hall Cross Academy utilises Smoothwall as firewall protection and web filtering for internet connections. Sophos endpoint protection is on all Academy devices, to defend against malicious virus and malware attacks. The Data Disaster Recovery policy will be implemented as soon as the IT Team are made aware of an attack.

Two factor authentication is enabled for Hall Cross staff using cloud services, including email and cloud storage.

### **Electronic Hardware**

All hardware held within the Academy should be included on the asset register.

When an item is replaced, the register should be updated with the equipment removed and details of the new item.

Do not let anyone remove equipment unless you are sure that they are authorised to do so.

Staff issued devices should be kept with you where possible and secured when in the Academy.

In non-secure areas, consider using clamps or other security devices to secure laptops and other portable equipment to desktops.

Staff laptops that are taken off site have Bitlocker Drive Encryption activated.

### **Home Working Guidance**

If staff must work outside of the Academy or at home, this presents increased risks for securing information. The following additional requirements apply:

- Do not access confidential information when you are in a public place, such as a train and may be overlooked;



- Do not have conversations about personal or confidential information on your mobile when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people;
- If you use a laptop, tablet or smartphone, ensure that it is locked and password protected to prevent unauthorised access;
- Make sure that you don't leave your device anywhere it is more likely to be stolen;
- When working on confidential documents away from the Academy, do not leave them lying around where others may see them; dispose of documents using a shredder;
- Electronic devices/confidential information must not be left in cars overnight; and
- If you are using your own computer, ensure that others cannot access documents. It is forbidden to use a computer owned by you to hold personal data about pupils or staff at the Academy.

### **Audit of Data Access**

Where possible our software specifications will include the function to audit access to confidential data and attribute access, including breaches of security, to specific users.

### **Data Backup**

The Academy will arrange that all critical and personal data is backed up to secure on-line (off physical site) storage. If the Academy is physically damaged critical data backups will allow the Academy to continue its business at another location with secure data.

Data backup should routinely be managed on a daily basis to secure off-site areas.

### **Sharing of Personal Information**

The Academy only shares personal information with other organisations where there is a legal requirement to do so or the organisation has been contracted by the Academy to carry out a function of the Academy.

The Academy is required, for example, to share information with the Department for Education and the Education Skills Funding Agency. Under certain circumstances, such as child protection, we may also be required to share information with Children's Social Services or the police.

All pupils have a right to access their own personal information held by the Academy. Where the child is below the age of 16 years this will be exercised through their parents or guardians.

The Principal will be responsible for authorising the sharing of data with another organisation.

The Principal, in authorising the sharing of data will take account of:

- Whether it is lawful to share it;
- Whether there is adequate security in place to protect the information while it is being transferred and then held by the other organisation;
- Ensuring the Privacy Notice includes a simple explanation of who the information is being shared with and why;
- Considerations regarding the method of transferring data, which should include:



- If personal data is sent externally by e-mail, then security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending the message. The data must be encrypted and the password sent separately. You must also check that it is going to the correct e-mail address.
- Circular e-mails sent to parents should be sent bcc (blind carbon copy) so that the e-mail addresses are not disclosed to everyone.
- If confidential personal data is provided by paper copy it is equally important to ensure that it reaches the intended recipient.
- If consent has been obtained to share data which is not a legal requirement to do so.

## **Breach of any Requirement Under GDPR**

Any breach of data protection must be reported immediately to the Data Controller for the Academy (via email at [dpo@hallcrossacademy.co.uk](mailto:dpo@hallcrossacademy.co.uk)), providing as much detail on the breach as possible i.e. when did it take place, what data has been breached, what actions you have taken to rectify the breach.

Once notified, the Data Controller shall assess:

- The extent of the breach;
- The risks to the data subjects as a consequence of the breach;
- Any security measures in place that will protect the information;
- Any measures that can be taken immediately to mitigate the risk to the individual(s); and
- Report breaches to the Data Protection Officer in the Academy.

If the Data Protection Officer concludes that there is likely to be a risk to the rights or freedoms of individuals from the breach, it must be notified to the ICO within 72 hours of the breach having come to the attention of the Academy, unless a delay can be justified.

The Information Commissioner will be told:

- Details of the breach, including the volume of data at risk, and the number of categories of data subjects;
- The contact point for any enquiries (the Data Protection Officer);
- The likely consequences of the breach; and
- Measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Data Protection Officer shall notify data subjects of the breach without undue delay; unless data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data Subjects shall be told:

- The nature of the breach;
- Who to contact with any questions; and
- Measures taken to mitigate any risks.

The Data Protection Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any

recommendations for further training or a change in procedure shall be reviewed by the Accounting Officer and a decision made about implementation of those recommendations.

## **Policy Review and Development**

This policy will be reviewed every two years by the owner, the Principal and the GDPR Team.

## Document version change control

Version:	Date:	Details of changes:
1	02/12/19	N/A
2	29/11/21	<p>Additional information included under the following headings:</p> <ul style="list-style-type: none"><li>● Conditions for processing in the first data protection principle</li><li>● Data Controller</li><li>● Notification with the Information Commissioner's Office (ICO)</li><li>● Definitions</li><li>● Disclosure of personal information to third parties</li><li>● Why we collect information</li><li>● Information security</li><li>● Sharing of personal information</li><li>● Breach of any requirement under GDPR</li></ul>

## Appendix/Appendices

### The General Data Protection Regulation (GDPR) 2018

This came into force in May 2018. The purpose of GDPR is to protect the individual rights and freedoms of individuals, especially their right to privacy with respect to the processing of personal data.

GDPR applies to personal data (information that applies to a living person) whether it is held on a computer system or on paper. There are particularly stringent rules surrounding 'sensitive' data such as pupil identifiers, pupil characteristics, special educational needs, health, religious beliefs, ethnic background, home address and criminal offences.

Personal data can only be processed under one or more of the following rules:

- An individual has given consent
- It is part of a contract
- It is a legal obligation
- It is necessary to protect the individual
- It is in the legitimate interests of the data controller

Every item of personal data that is held or processed must be accurate and up to date, and held for no longer than necessary. When data is no longer relevant to the purpose for which it was originally obtained, and/or has reached the end of the period for which it must legally be retained, it must be destroyed in accordance with the relevant Impact Level of the data.

The security of personal information must be maintained and any disclosure of personal data must be properly authorised. There are specific consent requirements in respect of data transferred to countries outside the European Economic Area.

It is a legal requirement to protect sensitive data. Individuals entrusted with this data, however derived, are accountable for the protection and compliance with GDPR.

## Glossary

<b>Antivirus Program</b>	A utility that searches storage devices for viruses and removes any that are found. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered.
<b>Backup</b>	To copy files to a second medium (a disk or tape) as a precaution in case the first medium fails.
<b>Confidential</b>	Classification for documents that are only available to members of Hall Cross Academy that they are relevant to or to whom they are directly sent.
<b>Data</b>	Any information that is stored either digitally or in printed/written format and maybe/is used to identify any individual or group, or may be deemed to be sensitive in nature.
<b>DPA</b>	Data Protection Act 2018
<b>Encryption</b>	A process which is applied to text messages or other important data, and alters it to make it humanly unreadable except by someone who knows how to decrypt it.
<b>Encryption Software</b>	Software whose main task is encryption and decryption of data, usually in the form of files on (or sectors of) hard drives and removable media, email messages, or in the form of packets sent over computer networks.
<b>GDPR</b>	The General Data Protection Regulation (GDPR) 2018.
<b>Group Policy</b>	Provides centralised management and configuration of our Operating Systems.
<b>Help Desk</b>	Provides information and assistance to the users of the school's ICT systems.
<b>IAO</b>	Information Asset Owner
<b>ICO</b>	Information Commissioners Office
<b>ICT</b>	Information and Communications Technology.
<b>ICT Systems</b>	All computer and related systems within the school environment and also encompasses non computer based communication systems including TV, telephone etc.
<b>ICT Systems Manager</b>	Person with overall responsibility for the school's admin and curriculum networks.

<b>Incremental backup</b>	Backup in which only the data objects that have been modified since the time of some previous backup are copied.
<b>Internal</b>	Classification for documents, that are available to all members of Hall Cross Academy.
<b>MIS</b>	Management Information System (SIMS).
<b>Network Cabinet</b>	Also known as a rack. A metal frame used to hold various hardware devices such as servers, hard disk drives, modems and other electronic equipment.
<b>Portable and mobile devices</b>	Any computing or communications device intended to frequently move location while maintaining function and operation, e.g. A mobile/smart phone, laptop computer etc.
<b>Public</b>	Classification for documents, that are available to members of the public and are published on the Academy website.
<b>SIRO</b>	Senior Information Risk Owner.
<b>Staff</b>	A person employed by Hall Cross Academy.
<b>UPS</b>	A unit that switches to battery power whenever the mains power cuts out and allows time for ICT systems to be properly shut down or to continue to function until mains power is restored.
<b>Users</b>	Anyone that makes use of the ICT systems
<b>Virus</b>	A computer program that can copy itself and infect a computer. The term "virus" is also commonly but erroneously used to refer to other types of malware, including but not limited to adware and spyware programs that do not have the reproductive ability.
<b>WSUS</b>	Windows Server Update Services