School Policies

Policy title	Data Management Policy

Written on	May 2015	Reviewed on	April 2017	Next review due	April 2018
SLT link	Dean Barnett		Governor link		

Copies in	Policies folder √	Handbook	Student planner	Website

DATA MANAGEMENT POLICY

The purpose of this policy is to look at the data protection within Crown Hills Community College and to make aware to all users what is required regarding the processing and collecting of Personal data relating to learners and other individuals. The lawful and correct treatment of personal information by Crown Hills Community College is very important to successful operations, and to maintaining confidence between those with whom we deal and ourselves. The Governors, Principal and nominated Senior Information Risk Owner, (Business Manager and Vice Principal) and all staff will ensure that our organisation treats personal information lawfully and correctly and is only made available for those who are authorised to access it. We fully endorse and adhere to the principles of data protection detailed in the Data Protection Act 1998. **All staff within Crown Hills Community College are responsible for the security of data.**

Personal data is anything which identifies anyone as an individual, either on its own or by reference to other information. It can include expressions of opinion about someone.

The Data Protection Act 1998 applies only to personal data about a ***living, identifiable individual.***

The Data Protection Act 1998 states all schools processing personal data must comply with the eight enforceable principles of good practice.

These are as follows:

1. **Data must be fairly and lawfully processed**
2. **Data must be processed for limited purposes**
3. **Data must be adequate, relevant and not excessive**
4. **Data must be accurate**
5. **Data must be not kept for longer than necessary**
6. **Data must be processed in accordance with the data subject rights**

7. **Data must be secure. Measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.**
8. **Data must not be transferred to other countries without adequate protection.**

In order to comply with these principles we should adhere to the following when processing personal data.

1. **Observe fully conditions regarding the fair collection and use of information.**
2. **Collect and process appropriate information, and only to the extent that is needed.**
3. **Ensure the quality of information used.**
4. **Apply strict checks to determine the length of time information is held. Please refer to the Retention guidelines for local government. Copy can be found with the SIRO.**
5. **Ensure that the rights of people about whom information is held, are able to be fully exercised under the Act. (These include: the right to be informed that processing is undertaken, (Privacy Notice) *Please see below***
6. **The right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct rectify, block or erase information which is regarded as wrong information.**
7. **Ensure that information is not transferred abroad without suitable safeguards.**
8. **Meet its legal obligations to specify the purposes for which information is used.**

As a minimum a privacy notice will be sent to all parents/carers when the student starts at Crown Hills Community College and also directly to the student when they reach the age of 13.

In order to maintain data within the realms of the Data Protection Act we will ensure that the data held about a student or individual is correct.
Crown Hills Community College will issue a data sheet setting out what data is held and what additional data is required.
If Crown Hills Community College intends to share any data outside the parameters of the privacy notice we would only do so if such sharing complied with the Data Protection Act 1998 and that such organisations were described and included on the privacy notice.

Crown Hills Community College will conform to the requirements of the Data Protection Act (1998) by formally notifying the Office of the Information Commissioner annually:

- The purposes for which the school holds personal data
- What data it holds
- The source of the data
- To whom the data is disclosed
- To which countries the data may be transferred.

FREEDOM OF INFORMATION ACT 2000

This Act will give a general right of access to all types of recorded information held by Crown Hills Community College, but with exemptions. The two main responsibilities under the Act for Crown Hills Community College are:

- Will produce a 'publication scheme' of the information that is held and which is publicly available.
- Will deal with individual requests for information.

RETENTION SCHEDULE

Under the Freedom of Information Act 2000 Crown Hills Community College will maintain and review when appropriate the retention schedule listing that will show the length of time in which records will be retained and manage all current record systems using this retention schedule. The schedule refers to all information, regardless of the format in which it is stored. When obsolete records or a series of records are identified which contain personal information or anything that could be seen as sensitive, including policies, Crown Hills Community College will be committed to shredding such documents before disposal.
All other records for destruction will be disposed of using the locked confidential waste containers found in each zone.
All retained information that is destroyed will require the following record to be kept within a central Excel spreadsheet held by each head of department.

- Date and time it was destroyed.
- Who authorised the destruction of the information that was held.
- File Reference of document or unique identifier of such piece of document.
- File tile. (This will be a brief description of the document)
- The number of files.

ARCHIVES

Where records have been identified by individuals as to being worthy of permanent preservation, arrangements will be made with the ICT managed service contractor Capita, to transfer the records to the Archives. This

information will also be saved centrally with the information above. All paper information which has a lengthy retention period, in excess of 8 years or is being permanently archived can be considered for converting to media files.

All employees of Crown Hills Community College have recognised the importance of the following data protection guidelines that are set out in accordance with the Data Protection Act 1998 and also the Crown Hills Community College data Policy.

E-Safeguarding is the responsibility of all staff to assure that all information is kept confidential. Government guideline classifications will be implemented to restrict any such breaches of information confidentiality:

- RESTRICTED. Personal information related to pupils or staff (usually contained in the Management Information System) will only have access by authorised named users or groups. The decision of restricted information will be made by the Principal/Senior Team/SIRO (Senior Information Risk Owner).
- PROTECTED. School routines, schedules and management information, which is not expected to be released to the general public.
- PUBLIC. Website and promotional materials including newsletters, plus display around the school which is available for anyone.

All ICT equipment must be disposed of so that all the personal data on the device is removed by an official contractor that will provide a warranty that ensures the user that they have securely erased all the disks.

It is essential that personal data including passwords and email are not just deleted as this is not sufficient under the Data Protection Act 1998. Staff must consult the ICT technician or Capita before any disposal can take place.

ACCESS TO ICT

- All access must be via a unique username and password. This should not be distributed to any other person. There will be no exceptions to this unless a risk assessment has been approved by the senior information risk officer. Usernames are held centrally by the ICT Managed Service Provider. If you have concerns that this information may be known please see ICT Technician.
- Information storage will be managed by the approved users and centrally held on Capita Servers. Please refer to Capita's data Control Policy relating to how they handle school data.
- External users can only access information with authorisation from the Principal/SIRO
- All requests for access beyond that normally allocated (e.g. teachers wishing to access pupil personal storage) shall be authorised by the SIRO. This shall include the authorisation of access required by the ICT Support Team during investigations.

- Where restricted information is stored access will only be granted by the Principal/SIRO.
- All users that leave the employment of Crown Hills Community College will have their access removed.
- All users will take responsibility and take all necessary steps to ensure that they use the technologies available to them safely, legally and responsibly.
- All Internet activity should be appropriate to staff professional activity.
- Activity which threatens the integrity of the college ICT systems, or activity that attacks or corrupts other systems, is forbidden
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright law of materials must be respected.
- Posting anonymous messages and forwarding chain letters is not permitted.
- As e-mail can be forwarded or inadvertently be sent to the wrong person the same professional levels of language and content should be applied as for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or offensive materials is forbidden
- Crown Hills Community College reserves the right to examine or delete any files that may be held on its computer system or monitor any Internet sites visited
- Where possible, the use of memory sticks and other mobile storage media should be restricted, or scanned for viruses each time they are connected.
- A secure network is provided within the school. Third party access will only be enabled following authorisation of the SIRO.

PASSWORD SECURITY

All members of staff will take responsibility for creating their own password which will not be discussed with any other member of staff, student, friend or family member.

These appropriate steps should be followed to safely select a secure password:

- Always use a different password for school ICT devices to the one that is used for personal home use ICT equipment.

- Always create a password that is difficult to be viewed by others when logging into the device.
- Make your password at least 8 characters long using letters, numbers and characters (*^@Clock211) amongst a word or name that you will remember.
- Change passwords at least at the start of every term.
- Do not write down your password or log in details related to any device.
- All school mobile phones must have at least a secure 4 digit password that automatically locks the phone 1 minute after use for protection.
- Any software packages that are owned by a department that may require a password and log in, e.g. Schoolbooking.com should be closed down when not in use to avoid unauthorised access.

INCIDENTS

Following any breach it is important to report promptly so that the Principal/SIRO/LCC can assess whether it needs to go to the Information Commissioner's Office:

- All e-safety and personal data incidents should be reported to the Principal immediately. This should include the date of the incident and any information that may have been compromised from the occurrence.
- Any breach that you may be aware of from student use should be reported immediately to the Vice Principal Key Stage Manager of that year and also the ICT technician. Any investigation that needs to take place by the ICT technician will have authorisation in writing and the person conducting the investigation will have a member of the SMT present, so to protect that person doing the investigation.

WORKING AWAY FROM SCHOOL

When using mobile computing devices and connecting to the schools MLE network from home the following must be adhered to:

- Only necessary information should be stored on the device.
- Pupil sensitive (restricted) information shall not be stored on any mobile devices unless encrypted. Restricted information is personal or sensitive information relating to staff.
- Memory sticks that are not encrypted should not be used for any sensitive or personal data.
- iPods/ iPads should only contain necessary information and be locked at all times whilst they are not in use.

- All laptops are the responsibility of all staff to safeguard the device from theft, loss, damage or while the device is in transit to or from home or off site.
- Individual will be responsible for preventing unauthorised access.
- It is strongly advised that you do not use MySchool on any public computers as the security and settings on these are often unknown and may be actively insecure.

SECURITY AND STORAGE OF DATA

Physical security of data is maintained and managed by Capita but the actual property of the data is the responsibility of Crown Hills Community College. Therefore the following guidelines should be adhered to:

- When leaving your computer or laptop unattended lock the computer using CONTROL, ALT, DELETE
- Passwords should not be removed from any device which may have sensitive or personal data on. This includes mobile phones.
- Personal laptops, home computers, android devices, iPADS and mobile phones should not be used for the storage of any sensitive or personal DATA.
- Always use your school email address for work related information that you receive or send. When sending email mark as confidential if required. You may also consider using the message options to add:
- Importance
- Sensitivity
- Delivery and Read receipt
- Information Manager rights which sets permissions.
- No forwarding of emails to personal addresses allowed in any instance unless prior consent has been given by the Principal or SIRO.
- Always remove sensitive data from your inbox of your outlook account and save to a relevant folder in your user area.
- Only use encrypted laptops and memory sticks for all files that contain personal, sensitive, confidential or classified information.
- Alert the Principal or Line Manager at once if you have lost or had your mobile phone or mobile device stolen. This should also be reported to the ICT technician (CHCC) so the device can be remotely blocked.
- Ensure all hard paper copies of staff and student's sensitive or personal data including confidential and classified documents are filed securely and not left out in classrooms or offices when unattended by those responsible for the data. If these documents are no longer required they

must be disposed of in the correct manner. (Refer to retention schedule section of this policy)

- Ensure all data is correctly labelled.
- Ensure that any hard copies of confidential data are not removed from site. If this is required for work related purposes then this data must be transported securely and stored safely off site when removed from the school.
- Ensure the fax machine is not used for sending or receiving any sensitive, personal or confidential data. It may not be picked up at either end by the person it was intended for.
- Particular care should be taken when leaving devices in cars ensuring that they are not visible. Lock away in the boot of the car.
- Any DVD'S, CD's OR CAMERA MEMORY DEVICES that may have been used for sensitive or personal data including photos should be stored correctly in a locked cupboard. If these need to be disposed of please contact the ICT technician.

THE NETWORK

Although the school infrastructure is the property of Leicester City Council and the school the data held is managed and maintained by the ICT Service Provider. All security and software updates including antivirus protection will be part of the provision.

For further information please refer to the Managed Service provider, Capita's data handling Policy and service provision.

As a user of the College ICT equipment, Internet, email and all associated software packages used within my employment at Crown Hills Community College I agree to comply with the written Crown Hills Community College Data Protection Management Policy and work within the legal framework of the Data Protection Act 1998 on the safe and secure use of handling data.

Signed; **Date:**