Horizon Community College Information Governance Policy

Inclusive of:
Acceptable use, CCTV Code of Conduct, Data Proteection Act 2018 (DPA), Freedom of Information Act, General Data Protection Regulation (GDPR), Information Security, Online Security, Paper Records Policy, SIMS Management

To be read in conjunction with Safeguarding and Child Protection Policy and HCAT Data Protection & GDPR Policy

Reviewed:
November 2023

Ratified:
November 2023

INFORMATION GOVERNANCE POLICY

CONTENTS

Section 1 General Policy Agreement

Horizon Community College has a duty of care to its governors, staff and students that are using ICT and related technologies both on and off the college premises.

The Principal and Governing Body of Horizon Community College recognise their responsibilities in ensuring that the systems accessed by all parties are safe, secure, monitored, and managed appropriately.

They will ensure that the college complies with the Data Protection Act 2018 and the General Data Protection Regulation, to ensure that the College Information Management System in respect of staff and student data is kept safe and secure in line with relevant legislation at that time.

They will agree a policy that the college fulfils its responsibilities in respect of the statutory guidance for Information Governance.

This policy document will be reviewed on an annual basis and ratified at a full governors meeting.

Section 2 Information Governance Policy Statement

Information Technology has become integral to the lives of people, including children and young people of today's society, both within and outside of their college lives. The Internet and other digital technologies are powerful tools, which open up a vast array of new opportunities for everyone.

These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective teaching and learning. Everyone including children and young people should have an entitlement to **safe** access to technology and the Internet. Horizon Community College is committed to ensuring that all information utilised or created within the college is appropriately controlled, used and managed to assure compliance with relevant legislation at that time. This policy is designed to support the governors, staff, students, visitors, contractors and any third parties to ensure that information which is classified as being restricted or confidential is not divulged to any person or organisation outside college who are not authorised for access.

It applies to all governors, staff, students, visitors, contractors and any third parties where they are operating on behalf of the college and wherever that may be, both their normal place of work or elsewhere such as at home, when accessing information which the college is responsible for.

In this context, information includes that held on both physically (paper) and electronically stored on computers, servers, external media such as but not limited to; cloud storage such as OneDrive and SharePoint, physical media such as disc, USB media and external hard drives, mobile telephones or other media. Information held by the College is managed against the same standards regardless of the media in which it is stored.

This policy applies to all information except un-restricted public information.

Section 3 Duties

3.1 The Horizon Local Committee (HLC)

The HLC will:

- Agree a policy ensuring that the appropriate arrangements are in place to ensure compliance
- Ensure that the college has the resources to implement the policy and that these are used appropriately
- Appoint a link HLC member (formerly known as governors) who will monitor the implementation of the policy and review and present the policy to thr HLC for ratification on an annual basis

3.2 The Principal

The Principal is responsible for ensuring:

- That the college has in place; systems, procedures and appropriate staffing to ensure that all computer use is carried out in accordance with the policy
- That members of staff are allocated to specific roles for the management and implementation of this policy

- That the effectiveness of this policy is monitored and that the Governing Body are kept fully informed

- That investigation of and reporting of any data breach or information loss (either lost or stolen) particularly loss of computer equipment and mobile data devices is reported to the appropriate authorities. This responsibility has been delegated to the Data Protection Officer (DPO)

3.3 The Associate/Associate Vice Principals

The Associate Principals will undertake the role in the absence of the Principal and will undertake the Information Governance responsibilities as required.

The Associate Vice Principal – Quality of Education is the link to the Principal's Team in respect of ICT.

3.4 The Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for:

- Ensuring that the college is compliant with all aspects of The Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR)
- Overseeing the security, storage and archiving of paper records listed within the relevant section and should effectively manage the processes by organising training, setting schedules and ensuring procedures are carried out, but will not always to be involved in the day to day administration of the process

3.5 The Digital Infrastructure Lead:

The Digital Infrastructure Lead is responsible for (and may delegate as appropriate):

- Making sure all users are aware of this policy

- Ensuring all staff understand and are aware of the policy, and adhere to it

- Ensuring that the technical infrastructure and network is as safe and secure as possible

- Updating the list of inappropriate websites which fall through the filtering software

- Maintaining up to date accurate records of policy compliance

- Maintaining up to date accurate records of staff or students who have access to systems externally

- Supporting the investigation of Online Safety incidents

- Applying sanctions to user accounts when necessary

- Reporting to governors on a termly basis, any breaches of Health and Safety issues relating to ICT

- Ensuring that appropriate training is undertaken before authorising access to the information systems

- Providing details of access permissions to enable all users (including temporary) to be connected to the network, allocated an email address and have access to information systems to the system administrator and to notify of any changes

- Providing Strategic support to the Data Protection Officer (DPO)

3.6 The Subject Leader for Computing is responsible for:

- Developing an Online Safety culture

- Acting as a named point of contact on all Online Safety issues for the college, under the guidance of the Principal

- Promoting the Online Safety vision to all stakeholders and support them in their understanding of the issues

- Ensuring that Online Safety is embedded within the continuing professional developments for staff and co-ordinate training as appropriate

- Ensuring that Online Safety is embedded across the curriculum and activities within the organisation as appropriate

- Ensuring that Online Safety is promoted to all stakeholders

- Supporting pastoral teams to decide on appropriate sanctions for students

- Monitoring and reporting on Online Safety issues to the management team, Trust and any other relevant agencies

- Developing an understanding of the relevant legislation

- Liaising with the Trust and other local bodies as appropriate

- Reviewing and updating Online Safety best practice and advise the Digital Infrastructure Lead

3.7 All staff are responsible for making sure :

- That they understand and comply with this policy

- That information they access in fulfilling their role is managed, processed and used effectively, securely and legally

- That they keep secure all information both paper based and computerised

- That they only access computer systems which they have been authorised to access, in an appropriate manner and for the agreed purpose

- That no one else uses their log in ID

- Their own passwords are kept secret and if breached are changed as soon as possible by contacting the IT Service Desk

- They do not store restricted personal data, or confidential information on mobile devices or local drives (C:\ drives on personal or college computers)

- They log with the IT Service Desk, any inadvertent misuse or inappropriate use of information

- They lock their computers if logged in when leaving the computer for any short period of time (a maximum of 10 minutes is advised)

- They log out the computer if logged in when leaving it for an extended period of time (more than 30 minutes is advised)

- That no email message containing restricted personal data or confidential information is forwarded to a personal email address
- That when viewing restricted or confidential information that due care is paid to restricting the screen from others

- That when discussing (either face to face or via telephone) confidential or restricted personal data they consider who could be listening

- That when working with information that the appropriate procedures are followed relative to the information value

3.8 All Students are responsible for making sure:

- They keep themselves safe when using ICT – in line with the Online Safety and Acceptable Use sections of this policy document

- They report any instances of intentional or non-intentional breaches to this policy to a member of staff

- They adapt good Online Safety practice using digital technologies both in and out of college

3.9 Visitors & Contractors are responsible for making sure:

- That they understand and comply with this policy

- That information they access whilst carrying out their duties is managed, processed and used effectively, securely and legally

- That they keep secure all information given, both paper based and computerised

- That they only access computer systems which they have been authorised to access, in an appropriate manner and for the agreed purpose

- That no one else uses their log in ID (if assigned)

- Their own passwords are kept secret and if breached are changed as soon as possible by contacting the IT Service Desk

- They do not store restricted personal data, or confidential information on mobile devices or local drives (C:\ drives on personal or college computers)

- They report any inadvertent misuse or inappropriate use of information to the IT Service Desk

- They lock their computers if logged in when leaving the computer for any short period of time (a maximum of 10 minutes is advised)
- They log out the computer if logged in when leaving it for an extended period of time (more than 30 minutes is advised)
- That no email message containing restricted personal data or confidential information is forwarded to a personal email address
- When viewing restricted or confidential information that due care is paid to restricting the screen from others
- When discussing (either face to face or via telephone) confidential or restricted personal data they consider who could be listening
- When working with information that the appropriate procedures are followed relative to the information value

Section 4 Data Protection

4.1 Data Protection

Horizon Community College adheres to the Data Protection Act 2018 and the General Data Protection Regulation (GDPR)

Reference to:

- https://www.gov.uk/data-protection

The Data Protection Act 2018 and General Data Protection Regulation controls how your personal information may be used by Horizon Community College.

Everyone responsible for using data has to follow strict ‘data protection principles’.

They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes

- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people’s data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

There is stronger legal protection for more sensitive information, such as:

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records

The Data Protection Act 2018 and the General Data Protection Regulation gives you the right to find out what information Horizon Community College stores about you.

You can write to us and ask for a copy of the information we hold about you. Please address your request to the ‘Data Protection Officer’ (DPO) of Horizon Community College.

Horizon Community College is legally required to give you a copy of the information that we hold about you if you request it.

When information can be withheld?

There are some situations when Horizon Community College are allowed to withhold information, for example if the information is about:

- the prevention, detection or investigation of a crime

- national security or the armed force

- the assessment or collection of tax

Horizon Community College doesn’t have to say why they’re withholding information.

How much it costs

Horizon Community College ***will not usually*** charge you for providing the information, however in some instances there may be a charge for certain types of information:

- certain types of records, such as health or education records

- a large number of paper records held in an unstructured way by us

Making a complaint

If you think your data has been misused or that Horizon Community College hasn’t kept it secure, you should contact the Data Protection Officer: DPO@horizoncc.co.uk

If you are unhappy with our response or if you need any advice, you should contact the Information Commissioner’s Office (ICO). ICO helpline telephone: 0303 123 1113

Horizon Community College is part of a Multi-Academy Trust (HCAT), therefore this section of the policy should also be read in conjunction with the Trust’s Data Protection and GDPR Policy – which can be located below:

https://www.hcacademytrust.education/key-information/policies-and-procedures/

Section 5 Information Security

5.1 Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords private and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and sign an agreement to demonstrate that they have understood the college's Information Governance Policy in place. A recording system is kept up to date by the Digital Infrastructure Lead of all staff's compliance, managed daily by the IT Network Manager

- Users are provided with a network and email account, which also provides access to the learning platform and Management Information System (MIS) automatically. They are also expected to use a personal password and keep it private

- Students are not permitted to deliberately access on-line materials or files on the college network or local storage devices of their peers, teachers or others

- Staff are aware of their individual responsibilities to protect the security and confidentiality of the college network, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. (Passwords are currently forced to change every 42 days via policy) Individual staff users must also make sure that workstations are not left unattended and are locked

- Due consideration should be given when logging into the college learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer)

- All ICT password policies are the responsibility of the IT Service Desk, and all staff and students are expected to comply with the policies at all times

5.2 Monitoring of Network Usage

The college and Trust are authorised to monitor, record and filter computer usage, without the consent of individual computer users in accordance with legislation and this policy. Non-compliance may result in appropriate disciplinary, contractual and/or criminal action being taken.

5.3 Breaches of Computer and Data Security

Everyone is responsible for notifying the Principal or their nominated representative if there is a breach of this policy and reporting:

- The nature and extent of the identified information loss

- Any incident or situation which may have a potential impact on the security of information systems

- Unintentional or intentionally access gained to unauthorised systems or information

- The identification of a system failure or weakness

All breaches of this policy will be treated as an issue of the utmost concern. Employees may be subject to disciplinary action. For deliberate and knowing breach of this policy where an information loss occurred or where a user is found to be abusing computer facilities then it will constitute potential gross misconduct. Each case of suspected misuse or non-compliance will be reviewed within the context and spirit of this policy.

5.4 Remote Access

- The college provides staff and students with the ability to work from remote locations such as home via the use of Microsoft 365 (SharePoint, OneDrive and other 365 services). Staff also have the flexibility to access Edulink One and MINTClass, which are linked to the college' MIS system, for data entry, planning and other similar tasks. **Please note** all sections of this policy apply to remote access systems whether on or off the college premises.

5.5 Social Media

Social media platforms are increasingly becoming an important part of our daily lives.

- The college uses Twitter to communicate with parents and carers. The nominated staff are responsible for all postings on this platform and monitors responses from others, under the guidance from the Digital Infrastructure Lead (a record of staff is retained by the IT Service Desk)

- Staff are not permitted to access their personal social media accounts using college equipment at any time during the college day

- Students are not permitted to access their social media accounts whilst in college

5.6 Telephones and Mobile Phones

- The use of college telephones and mobiles (where applicable) should be for college business only. No personal use of college telephony is permitted
- Where the college provides mobile technologies such as phones, laptop, tablets etc. for offsite visits and trips, only these devices should be used

- Where the college provides a laptop for staff, this device may only be used to conduct college business on

- Never use a hand-held mobile phone whilst driving a vehicle

5.7 Portable & Mobile ICT Equipment

This section covers items such as laptops, staff iPads's, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on college systems and hardware will be monitored in accordance with the Acceptable Use section of this policy

- Staff must ensure that all college data is stored on the college network (including Microsoft 365), and not kept locally on the laptop. Any equipment where personal data is likely to be stored must be encrypted

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car **before starting your journey**

- Synchronise all locally stored data, including diary entries, with the college network/servers (including Micorsoft 365) on a frequent basis

- Ensure portable and mobile ICT equipment is made available as necessary, to the IT Service Desk, for Anti-Virus updates, software installations, patches and upgrades

- The installation of any applications or software packages must be authorised by the Digital Infrastructure Lead, fully licensed and only carried out by the IT Service Desk – local device restrictions are in place to prevent this, to ensure the college is protected in relation to copyright breaches and other licence breaches that may result in penalties

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case, where supplied

5.8 Disposal of IT Equipment

- All redundant ICT or related equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive, General Data Protection Regulation (GDPR) and Data Protection Act (DPA). Approval from Governing Body will always be obtained before arranging a disposal collection with the relevant third party

- All documentation following a collection is retained by the Digital Infrastructure Lead for future reference. All redundant ICT equipment will be disposed of through an authorised agency. This should include a written or electronic receipt for the item(s), including an acceptance of responsibility for the destruction of any personal data

- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written or electronic guarantee to confirm this

Disposal of any ICT equipment will conform to:

- The Waste Electrical and Electronic Equipment Regulations 2013

- The Waste Electrical and Electronic Equipment (Amendment) (No.2) Regulations 2018

- Data Protection Act 2018

https://www.gov.uk/government/collections/data-protection-act-2018

- General Data Protection Regulation (GDPR)

https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

- Electricity at Work Regulations 1989

http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

The college will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

The college’s disposal record will include:

- Date item disposed of
- Authorisation for disposal, including:
    - Verification of software licensing
    - How it was disposed

Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate/sticker to identify this has been carried out.

5.9 'Sexting'

Keeping Children Safe in Education (KCSIE) statutory guidance sets out that all schools should have an effective child protection policy. Youth produced sexual imagery and a school's approach to it should be reflected in the policy. Please refer to Horizon's Safeguarding & Child Protection Policy for further information, a link to which is below:

https://horizoncc.co.uk/policies-and-reports/

Section 6 Staff, Student & Parent Responsibilities

6.1 Monitoring Online Safety

The college and Trust are authorised to monitor, record and filter online usage without the consent of individual computer users in accordance with legislation and this policy. Non-compliance may result in appropriate disciplinary, contractual and/or criminal action being taken.

6.2 Managing Online Safety

To ensure that all users understand the importance of Online Safety and their responsibilities in maintaining proper conduct online, the college will undertake the following actions:

- All stakeholders will be made aware of this policy and how it relates to them.
- All staff will sign the Acceptable Use Policy.
- Pupils will be instructed in responsible and safe internet use before being granted access.
- Responsible use of the internet, including social networking will be discussed through the Computing curriculum, assemblies and PHSE.
- To ensure sensitive and considerate monitoring of online usage, staff who operate monitoring procedures will be supported by the Digital Infrastructure Lead, Designated and Deputy Designated Safeguarding Leads.
- Staff training in safe and responsible internet use and on the contents of this policy will be provided as required.
- Parents will be regularly informed of their responsibilities in maintaining the Online safety of their child, with relevant information on issues covered by this policy made available.
- All stakeholders will be informed that cases of internet misuse by both students and staff, as well as other disciplinary breaches related to the policy will be dealt with through the college Behaviour, Anti-Bullying and Safeguarding and Child Protection Policies, as appropriate.
- All stakeholders will be informed that in cases of potential radicalisation/extremism The Prevent Duty will be implemented and could involve referral of individuals to the Prevent Duty Delivery Board and the Channel Panel.

6.3 Management of Filtering

- The College will work in partnership with parents, the DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- Any Internet user must report unsuitable/illegal sites to the Network Manager (and the Designated Safeguarding Lead if necessary) immediately.
- The Network Manager will oversee regular checks to ensure that the filtering methods used are appropriate, effective and reasonable. Content is filtered using ‘Smoothwall' ’ and communications are monitored through ‘AB Tutor’.
- If filtered websites need to be used by staff, they must inform ICT Technicians to have them unblocked for a set period of time (requests need to be approved by the Line Manager and/or IT Network Manager).
- Any Smoothwall alerts with severity rating 3 or above will be logged on CPOMs and where appropriate student and parents spoken to. Attempts to access inappropriate material may lead to a ban or a sanction.
- If there is a safeguarding concern as a result of the material searched then further safeguarding precautions will be taken to ensure the student's safety

Section 7 SIMS Management

7.1 Purpose

To provide and maintain a computerised database and to use the records to enhance and support the Teaching and Learning and administration of the college.

Records shall be kept for these specific areas in accordance with our registration under the Data Protection Act:

- Student Records – personal and academic
- Staff Records – personal and professional

The system may be used to help with the management of the following tasks:

- Staff cover
- Creating and running the timetable
- Profiles
- Options/Teaching groups
- Examinations
- Attendance
- External returns
- S.E.N.
- Recording Assessment
- Discover

7.2 Implementation

Responsibilities

The Systems Manager (Information Systems Manager) is to be responsible for the smooth running of the suite of SIMS programmes. To effectively manage the system but not to be responsible for its day to day application and use.

The named person will have a broad knowledge of the module and be responsible for its application and use:

- Personnel – Director of HR
- Staff INSET – Associate Principal
- Student Records – Information Systems Manager
- Academic Records – Information Systems Manager
- Timetable – Assistant Principal – College Systems
- Staff Cover – Assistant Principal – College Systems

- External Returns – Information Systems Manager
- Examinations – Assistant Principal – College Systems
- SEND – Assistant Principal – SENDCo

7.3 Procedures

- A nominated clerical officer will assist with the operation of each module and liaise with all concerned parties

- In all cases a second member of the clerical team will be familiar with the module to act as backup

Section 8 Acceptable Usage

8.1 Acceptable Usage

Acceptable usage is deemed as anything that is for the purpose or business of Horizon Community College and is to support the business in respect of Teaching and Learning or the administration function of the college. **Personal acceptable usage should be outside of normal working/teaching hours, i.e. before/after normal working/teaching hours or during any unpaid breaks.**

The following are acceptable personal usage:

- To organise an ad-hoc social activity on behalf of your department, or college

- Promotion of a charitable event

- To confirm a meeting with a colleague

- To confirm an urgent personal booking

- Shopping online (e.g. for groceries)

- Booking a holiday

- To read the latest news headlines

- Use to assist with a college sponsored course of study

- Use for research and development purposes, or other study course

- Preparation of CV's in connection with a job application

8.2 Non-Acceptable Usage

Illegal usage includes, but not limited to :

- National security – instructions on bomb making, illegal drug protection, terrorist activities
- Protection of minors – abusive form of marketing violence, pornography
- Protection of Human Dignity – incitement or promotion of racial hatred or racial discrimination
- Economic Security – fraud, instruction on pirating credit cards
- Information Security – malicious hacking
- Protection of Privacy – unauthorised communication of personal data
- Protection of Reputation – any form of libellous statement
- Intellectual Property – unauthorised distribution of copyrighted works e.g. software or music

Unacceptable usage:

It is unacceptable to utilise equipment, Internet or the e-mail system which

- is prejudicial to the college's interests
- is defamatory or abusive
- is for playing games (other than loaded as part of the standard system package)
- is for emailing games to others
- use of the college network and email function for declared business interests

Blocked Sites for the Internet

Access to a number of sites available on the Internet will be blocked by the IT Service Desk as follows: -

- Social Networking Sites (e.g. Facebook – dependant on role and requirement)
- Personal Messaging Systems (e.g. Facebook Messenger)
- Personal Trading (e.g. eBay)

8.3 Monitoring Acceptable Usage

The college has authorised the reporting on all aspects of information, computer systems, Internet and e-mail usage and the recording of usage of computer systems, e-mail and the Internet, without the consent of either the users or any other party to a transaction or communication and have the ability to report on inappropriate or excessive usage.

Compliance with this policy will be monitored on a regular basis through a range of measures including the use of e-mail filtering facilities, firewall protocols (Smoothwall) and reports analysing access and usage of Internet sites. Non-compliance may result in appropriate disciplinary, contractual and/or criminal action being taken.

Detailed personal analysis of Internet or e-mail usage will only take place where: -

- a concern arises from a service audit report or investigation
- general usage reports indicate an area of concern requiring further detailed investigation
- where there is a suspicion or allegation of inappropriate usage raised by the line manager or subject leader

8.4 Breaches of Acceptable Usage

Everyone is responsible for notifying the Principal or their nominated representive if there is a breach of this policy and reporting:

- Any incident or situation which may have a potential impact on the security of the network

- Unintentional or intentionally access gained to unauthorised systems or software

- The identification of a virus or system failure or weakness

- The user receiving an email message which contains unlawful, indecent or objectionable material

- A suspicion of inappropriate use of the internet or email by someone

All breaches of this policy will be treated as an issue of the utmost concern:

- Actions in response to staff breaches of Acceptable Usage will be in line with college/Trust HR and Safeguarding and Child Protection Policies Safeguarding and Wellbeing policies.

- Actions in response to student breaches of Acceptable Usage will be in line with the college Behaviour, Anti-Bullying and Safeguarding and Child Protection Policies.

- Each case of suspected misuse or non-compliance will be reviewed within the context and spirit of this policy.

Section 9 CCTV Code of Conduct

9.1 Purpose and Principles

This section has three purposes:

Purpose 1:

To ensure the legitimacy of the system and the use of recorded images at a later date. It is essential that the necessary criteria for operation be met.

Purpose 2:

To ensure that owners, managers and operatives know their roles and responsibilities when operating the system.

Purpose 3:

To ensure that the fundamental principles of the Data Protection Act 2018 and/or General Data Protection Regulation are met, and that the system is set up for correct operational procedures.

The principles of operating a CCTV system

Closed Circuit Television (CCTV) is a method of observing places and people, usually from a distance. It comprises of one or more cameras viewing a 'scene' and displaying that scene to a CCTV operator on a monitor screen. The images viewed may be recorded for later playback. This Code of Practice is concerned only with recorded images that can be retrieved on demand at a later date.

CCTV surveillance is an increasing feature of our daily lives. We might be caught on camera while walking down the high street, visiting a shop, bank or local council office. It is a highly useful tool for law & order operatives and for other purposes such as traffic monitoring. However it could intrude into our private lives. Therefore for the public confidence in CCTV systems to be maintained, as well as meeting legislative requirements, it is necessary to demonstrate tight control over the operation of CCTV systems.

It is highly likely that the purpose of a CCTV system is to capture images of individuals. Therefore, adherence to the Data Protection Act 2018 and General Data Protection Regulation (GDPR) will play a major role in the operation of any system. This document assumes this and is created with that legislative adherence as a major consideration.
Where images are 'real time' and not recorded then the Data Protection Act does not apply, but other legislation or policies may.

This document relates only to CCTV systems that Horizon Community College operates or has a controlling interest in.

It does not cover:

- Targeted and Intrusive Surveillance Activities which are covered by the Regulation of Investigatory Powers Act (RIPA)

- Use of surveillance techniques to monitor Horizon employees' compliance with their contracts of employment - if any such surveillance exists

- Security equipment installed in homes by individuals for home security purposes

- Use of cameras and similar equipment by the media for the purposes of journalism, or for artistic or literary purposes

The framework for a CCTV policy is based on:

- The legality of the CCTV system
- The training of managers and employees
- The set up and operation of the CCTV system, including Rights of the public with relation to recorded images

9.2 Documentation

The CCTV system installed at Horizon Community College is operated by Horizon Community College and the Facilities Management (FM) Provider, Amey Community Limited, for the following purposes -

- Safety and security of employees, students and visitors
- Security of premises during and outside normal working hours, car park monitoring
- Prevention, investigation and detection of crime

Note: The CCTV system will not be used for general surveillance of staff, pupils or visitors or for purposes not compatible with the purposes indicated above.

Definition of the person or organisation responsible for the system
Note: Breaches of the code by employees may constitute a matter of discipline under the relevant terms of employment.

Legal responsibility

- The organisation responsible for the CCTV system is Horizon Community College and Amey Community Limited includes: specifying system specification; ensuring legal conformity to installation and operation; representing the system in case of legal action being taken by plaintiffs
- The individual responsible for the CCTV system is The Principal of Horizon Community College. Legal responsibility will be in accordance with conditions of employment and Code of Conduct

Operational responsibility

- The Operation and System Manager is the Digital Infrastructure Lead as outlined in the grid in Appendix A

- Users of the system are the Digital Infrastructure Lead, all members of the College Leadership Team, along with further use by the College's School Teams, Student Wellbeing Officers and the Deputy Designated Safeguarding Leads. Outside of the College arena, the buildings Facilities Management (FM) provider, Amey Community Limited

- Authorised visitors, auditors and Trust representatives

- Relevant Health & Safety considerations shall be applied in accordance with current guidance or directive

- Where law enforcement organisations request control of the system (e.g. to mount a specific surveillance operation) then the CCTV Manager will ensure that s/he is satisfied as to the legality of the request and that appropriate documentation and controls are in force to maintain the basic operational principles of CCTV usage

9.3 Conformity with the Data Protection Principles

NOTE: Audio recordings that can be located (by date/time) and that can identify an individual, and that may be synchronised with image records (or available even if the images are not viewable) are classed as personal information and come under the Data Protection Act 2018. This document includes audio recordings in the terminology 'images'.

- The operation of this CCTV system, the procedures, staff training, and responsibilities are in accordance with the Data Protection Act 2018 and any policies of the Trust

- All the principles must be considered, and appropriate operational procedures put in place to meet those principles. A breach of any of the principles could result in an enforcement notice from the Information Commissioner, a fine, or both

- Where personal information may be exchanged either in bulk or on a regular basis then a Trust **Personal Information Sharing Charter** is recommended as the standard that all data sharing partners should abide by. Alternative data sharing agreements are acceptable providing they cover the Principles of the Data Protection Act 2018

- Such procedures and responsibilities are fully documented and available as part of management control, staff training, and on any request

- Signage must be displayed where an overt surveillance system is operated

9.4 Document the System Operation in support of its Legality

Siting the cameras to only cover those areas of legitimate concern.

- Cameras will be positioned so as to cover only the appropriate area of surveillance

- If this is not possible, then any other involved parties will be consulted

- If agreement cannot be reached the further advice (possibly legal) will be sought

Quality of the images

The CCTV system produces images adequate for the purpose for which it was installed and operates to the necessary level of efficiency.

Processing the images, conforming to the Data Protection Principles.

- Only authorised employees of the organisation will operate the system in accordance with the control procedures in force

- This includes recording of images and/or retained, further access to those images and staff training and responsibilities

Access to & disclosure of images to third parties must be for valid (and documented) reasons.

- Restricted access to image recordings, their disclosure to third parties and the quality of the images disclosed are subject to the organisation's policy which has reference to the Data Protection Principles

Access by Data Subjects - who have a basic right to information held about them, subject to certain exemptions.

- People whose images are recorded have the right to request a 'Subject Access Request'. It does not refer to people who request information that contains images of other people - that is a Freedom of Information request

- CCTV managers, operational staff and admin support staff must be able to recognise a Data Protection Subject Access Request (SAR) and pass to the relevant staff to action

Note: such a request may not be titled Data Protection, or may be incorrectly titled as Freedom of Information Request. We need to decide which it is and process the request according to the appropriate legislative rules.

Subject Access Request Process (Appendix B)

- Applicant must submit a request in writing. This could be their own written request, but it must contain the necessary information that facilitates the search for information e.g. images at a certain place, date and time

- Where the applicant wishes to complete the standard request form of the CCTV operating organisation appendix B document will be used

CCTV Maintenance Log. (Appendix D)

- CCTV equipment should be constantly monitored for effective operation and any problems reported immediately

CCTV System access – List of persons authorised to access the CCTV system. (Appendix A)

- This requires identification of specific persons authorised to access the system

- All listed persons must be in possession of this CCTV Code of Practice and have the facility to query any aspect of the CCTV operation they are not clear about

CCTV Viewing/Removal of Recorded Images. (Appendix C)

- All requests for access should be recorded, stating if disclosure has been made or not

Authorised Access List Appendix A

The following roles are responsible in the stated area of CCTV legality in support of its operational legality. This document also identifies persons authorised to access the CCTV system:

Role/Position	Responsibility
Principal	Data Controller
Data Protection Officer (DPO)	Data Controller
Digital Infrastructure Lead	Systems Manager
Premises Manager(s)	Amey Community Limited
Associate Principal(s)	Operator(s)
Vice Principal(s)	Operator(s)
Assistant Principal(s) inc. Head of School Role	Operator(s)
Head(s) of Year	Operator(s)
Student Wellbeing Officer(s)	Operator(s)
Safeguarding Lead(s)	Operator(s)
IT Service Desk Team	Operator(s)

Subject Access Request (SAR) **Appendix B**

HORIZON COMMUNITY COLLEGE
DATA PROTECTION ACT 2018
APPLICATION FOR SUBJECT ACCESS TO CCTV IMAGES

Data Subject's Name: ____

Address: ____

____ Postcode: _________________

Please provide the following information so that relevant CCTV images that may be held by the School can be located.

Date image was recorded: _____________________________________

Time (within 15 mins.): ______________________________________

NB. Disproportionate search time effort may invalidate the request

Location (e.g. Heart space, identified school) ______________________________

Please attach an appropriate photograph of yourself which will enable the operator to identify you on the CCTV images: (Staff with ID badges exempt)

Photograph provided □

Please tick the appropriate box

Do you wish to view the images or do you require copies?

View only: □ Copy required: □

Signature: ____________________________ Date: ______________________

Please return this form to the College

Guidance for Applicant

To enable your request for access to be processed promptly, please complete the form overleaf, providing as much information as you can.

You will be asked to provide satisfactory proof of identity e.g. driving licence, passport, recent correspondence addressed to you. The College may charge a fee.

If you are requesting access on behalf of another individual you will be required to provide written authorisation from the data subject. Any data found will be sent to the data subject.

Your Name: ____

Your Address: ____

____

_______________________ Postcode: ________________

In what capacity
are you acting? ____

Signature: _________________________Date: __________________

For office use only.

To be completed by the person receiving this application

Date form received on: _______________

by _______________________________

Identification submitted by applicant: ___________________ (type of identification)

Reference number of identification: ___________________

Fee receipt no: ________ (if collected)

Date: __________

Data Protection Officer Informed Date: __________

Section 10 Freedom of Information

10.1 Introduction

This is Horizon Community College's Publication Scheme on information available under the Freedom of Information Act 2000.

The governing body is responsible for maintenance of this scheme.

What a publication scheme is and why it has been developed.

One of the aims of the Freedom of Information Act 2000 (which is referred to as FOIA in the rest of this document) is that public authorities, including all maintained schools, should be clear and proactive about the information they will make public.

To do this we must produce a publication scheme, setting out:

- The classes of information which we publish or intend to publish
- The manner in which the information will be published; and
- Whether the information is available free of charge or on payment

The scheme covers information already published and information which is to be published in the future. All information in our publication scheme is available in paper form.

Some information which we hold may not be made public, for example personal information.

This publication scheme conforms to the model scheme for schools approved by the Information Commissioner.

10.2 Categories of Information Published

The publication scheme guides you to information which we currently publish (or have recently published) or which we will publish in the future. This is split into categories of information known as 'classes'. These are contained in section 6 of this scheme.

The classes of information that we undertake to make available are organised into four broad topic areas:

College Prospectus – information published in the College Prospectus

HLC's' Documents – information published in the HLC's' Annual Report and in other HLC documents

Students and Curriculum – information about policies that relate to students and the College curriculum

College Policies and other information related to the College – information about policies that relate to the College in general

10.3 How to Request Information

If you require a paper version of any of the documents within the scheme, please contact the College by telephone, email or letter. Contact details are set out below:

Email address: DPO@horizoncc.co.uk
Telephone: 01226 704230
Postal address: Horizon Community College, Dodworth Road, Barnsley. S70 6PD

To help us process your request quickly, please clearly mark any correspondence **"PUBLICATION SCHEME REQUEST"** (in CAPITALS, please).

If the information you're looking for isn't available via the scheme, you can still contact the College to ask if we have it.

10.4 Paying for Information

Information published on our website is free, although you may incur costs from your Internet Service Provider (ISP). If you don't have Internet access, you can access our website using a local library.

Single copies of information covered by this publication are provided free unless stated otherwise in section 6. If your request means that we have to do a lot of photocopying or printing or pay a large postage charge, or is for a priced item such as some printed publication or videos we will let you know the cost before fulfilling your request. Where there is a charge this will be indicated by a £ sign in the description box.

10.5 Classes of Information Currently Published

College Website – this section sets out information published in the College Website.

Class	Description
College Website	The statutory contents of the College website are as follows, (other items may be included in the website at the College's discretion): ▪ The name, address and telephone number of the College, and the type of College ▪ The names of the Principal, Chair of HLC and SENCO ▪ A statement of ethos and values ▪ Information on the College policy on admissions ▪ Information on School Uniforms ▪ Ofsted reports ▪ Key Stage 4 results from tests, exams and assessments for the previous academic year, as well as a link to the school and college performance measures website. ▪ College opening hours ▪ Curriculum information, including content of the curriculum the college follows in each academic year for every subject, including Religious Education. ▪ Remote Education provision ▪ Behaviour Policy ▪ Use of the Pupil Premium and Recovery Premium. ▪ Public Sector Equality Duties ▪ SEND Information Report ▪ Careers programme information ▪ Complaints policy and procedure

	▪ Annual financial reports and accounts, including details of executive pay ▪ Trustee’s information and duties ▪ Charging and Remissions policies ▪ How to obtain paper copies on request.

Policies and Reports – This section gives access to information about policies in regard to the college offer and responsibilities to all stakeholders.

Class	**Description £**
College Policies	▪ Assessment and Feedback ▪ Anti-bullying ▪ Behaviour for Learning ▪ Careers ▪ Charging and Remissions ▪ Curriculum and Teaching & Learning ▪ Drug, Alcohol and Illicit Substances ▪ English as an Additional Language ▪ Early Career Teaching ▪ Emergency Plan ▪ Equality (including Accessibility Plan) ▪ Examinations ▪ Healthy Eating ▪ Home Learning ▪ Information Governance ▪ Intimate Care ▪ Literacy ▪ Numeracy ▪ Remote Education ▪ RSHE ▪ SEND ▪ Uniform ▪ Work Related Learning
Trust Policies	▪ Attendance ▪ Administration of Medicines ▪ Complaints ▪ Data Protection and GDPR ▪ First Aid ▪ Health and Safety ▪ Financial Procedures and Regulations

	▪ Managing Parent and Visitor Conduct ▪ Pupil Premium ▪ Safeguarding and Child Protection ▪ Sexual Violence and Sexual Harassment Between Children ▪ Supporting Pupils With Medical Conditions ▪ Whistle Blowing ▪ Elective Home Education (Local Authority) ▪ Pay Policy
Reports	▪ SEND Information Report ▪ Pupil Premium Report ▪ Gender Pay Gap ▪ Trust Financial Statements

Our website address is: https://www.horizoncc.co.uk

10.6 Feedback and Complaints

We welcome any comments or suggestions you may have about the scheme. If you want to make any comments about this publication scheme or if you require further assistance or wish to make a complaint, then initially this should be addressed to:

The Data Protection Officer, Horizon Community College, Dodworth Road, Barnsley, S70 6PD.

If you are not satisfied with the assistance that you get or if we have not been able to resolve your complaint and you feel that a formal complaint needs to be made, then this should be addressed to the Information Commissioner's Office. This is the organisation that ensures compliance with the Freedom of Information Act 2000 and that deals with formal complaints. They can be contacted at:

Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Or;

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number

Fax: 01625 524 510

Website: www.ico.org.uk

Section 11 Paper Records

11.1 Specific Responsibilities

The named person will have a broad knowledge of their area and be responsible for looking after the associated paper records.

- ***Student Records – Assistant Principal – College Systems***
  Name, Address, Contact details for parents, DOB, attendance, behaviour etc

- ***Academic Records - Assistant Principal – College Systems***
  Assessment data, Exam results etc

- ***External Returns - Assistant Principal – College Systems***

- ***Personnel Records – HCAT Director of Human Resources***
  Personal - Name, Address, Contact details, Next of Kin, DOB etc.
  Professional - HR records

- ***Financial Records – Director of Finance***
  Invoices, bank statements, purchase orders, financial returns

Where it is necessary to retain hard copies of documents, these managers have overall responsible for the archiving of records within their area. They will supply staff with the necessary information and paperwork for use in the recording of documents which will be transferred into storage, along with the specific boxes needed for archiving. They are also responsible for ensuring documentation can be retrieved from storage upon request from staff.

Archiving will be undertaken at least once a year with documents stored on site in a secure storage room. Access to the room will be controlled by The Assistant Principal – College Systems, HCAT Director of Human Resources and Director of Finance, and retrieval of information will be coordinated through them. The room can not be opened by SS or GS keys, so staff other than those listed above, can not gain access to the archive room.

All staff are responsible for making sure:

- That they understand that records for which they are responsible for are accurate and are maintained and disposed of in accordance with the College guidelines and the data retention schedule. Seeking guidance from the Administration Manager when required

- That information they access in fulfilling their role is managed, processed and used effectively, securely and legally

- That they keep all information secure. Staff responsible for handling confidential paper documentation should take appropriate measures to avoid their unauthorised disclosure. This may involve locking the documents away when they are unattended. While confidential documents are being printed or copied, devices and documents must be either physically secure or else remain attended

- Staff should avoid the removal of hard copy documentation from the College premises. If records are removed from College, they must never be left unattended outside of college premises or in vehicles overnight. Any loss of college documentation must immediately be reported to the DPO

11.2 Record Keeping Systems

Maintenance of Record Keeping Systems

- It is important that filing information is properly resourced and is carried out on an annual basis. Files should be checked for any extraneous information where appropriate on a regular basis. Information held for longer than is necessary carries additional risk and cost. Records and information should only be retained when there is a business need to do so. Under GDPR, personal data relating to individuals must not be retained for longer than is necessary for its lawful purpose. Removing information from a file once a Freedom of Information request has been made is a criminal offence (unless it is part of normal processing)

- Applying retention periods is straightforward, provided files are closed on a regular basis. A retention schedule provides the length of time records should be retained

- Once a file has been closed it should be moved out of the current filing system, packed and labelled appropriately ready for archiving in the College's secure archive room

- Information security is very important especially when dealing with personal information or sensitive policy information. There are a number of basic rules:

- All personal information should be kept in lockable cabinets which are kept locked when the room is unattended

- Files containing personal or sensitive information should not be left out on desks overnight

11.3 The Safe Disposal of Information using the Retention Schedule

- Records should be disposed of in line with the approved retention schedule. This is a process which should be undertaken on an annual basis during the month of July/August for both academic and financial data

- Paper records containing personal information which can be destroyed, should be shredded using a cross-cutting shredder

Section 12 Glossary

ICT	Information Communication Technology
CCTV	Closed-Circuit Television
ICO	Information Commisoner’s Office
DPA	Data Protection Act
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
HR	Human Resources
PAT	Portable Appliance Testing
SIMS	School Information Management System
MIS	Management Information System
WEEE	Waste, Electrical and Electronic Equipment