Acceptable of ICT

Co-ordinator	**Business Manager**
Date of Completion	**August 2020**
Date of adoption by Governors and Trustees	**August 2020**
Date to be reviewed	**Every two years**

Contents

1. Policy Ownership and Responsibilities

1.1. The Governors of Downs View School and Link College and the Trustees of Downs View Life Skills College (DVLSC) have adopted and implemented this policy which relates specifically to Downs View employees.

1.2. The Use of ICT policy should be issued as part of the Rights and Responsibilities document given to all new staff. It should be read before using any ICT services. Failure to comply with the policy could lead to disciplinary action being taken against the employee, which could lead to dismissal, and in some cases legal action.

1.3. Employees are responsible for maintaining their awareness and complying with this policy and the Headteacher is responsible for monitoring compliance.

1.4. Any employee discovering a breach of this policy, or who is in receipt of an email or telephone call that appears to contravene the policy described below, should raise the issue with their line manager or the Headteacher in the first instance. Where the concern or issue persists and cannot be resolved, the Headteacher may escalate the matter to the Chair of Governors and/or the Executive Director - Families Children & Learning at Brighton & Hove City Council (BHCC), or the Chair of Trustees for DVLSC.

1.5. An employee who is subject to this policy and uses ICT services will be deemed to have consented to the monitoring and surveillance of email, their internet usage and workstations.

1.6. Please address any issues or concerns about this document to the Headteacher.

2. Terms Used in this Document

2.1. The following terms are used in the document:

- "must" means that any failure to comply is a serious breach of the policy;
- “should" means that compliance is strongly recommended but non-compliance may be acceptable in exceptional circumstances;
- "document" refers to either one or more electronic files used to record information in a loosely structured format;
- "database" refers to either one or more electronic files used to record information in a highly structured format;
- "computer system" refers to any combination of computer hardware, computer software and data that can be considered a discrete system; "workstation" refers to any desktop, laptop or tablet;
- "ICT" refers to Information Communications Technology;
- “employee" refers to any permanent, temporary or part time employee, or casual worker, at Downs View (contract staff should be covered by the same policy in their contractual agreement);

- "Council" refers to Brighton & Hove City Council.

3. Purpose

3.1. The purpose of this policy is to ensure that employees who use ICT services, do so in accordance with Downs View's business objectives and values. This will assist us in protecting employees from inappropriate use of technology, protect the security of information held on systems and limit the opportunity for fraudulent use of technology.

3.2. This policy is also intended to set out good practice for communicating, storing and retrieving information.

4. Scope

4.1. This policy applies to all Downs View employees. It is based on the Council's corporate Use of ICT policy. Relevant sections of this document should also form part of a contract for services for agency or contract staff.

4.2. Controlled use of ICT relies on a combination of responsible behaviour by users and the implementation of security features by ICT management and system owners. The scope of this policy does not extend to the latter but refers only to the responsible use of ICT by employees.

4.3. Certain staff working for Downs View or the Council's ICT teams may be exempted from some areas of this policy in order for them to carry out their normal duties. This only applies to staff who have been nominated as exempt by the Headteacher/Executive Director with the details of their exemption specified.

5. General Policy

5.1. Employees must not use any ICT services for copying, storing, sending or retrieving unacceptable material. "Unacceptable material" includes any documents, messages, information, graphics or other electronic data that:

- breach UK legislation
- contravene Downs View's Equality Policy;
- contain offensive, pornographic or obscene language or material
- plan, promote, incite or facilitate any illegal or terrorist activities
- contain defamatory or slanderous language or material
- denigrate, insult or ridicule another person
- intimidate, bully or harass another person
- adversely comment on the integrity, personality, honesty, character, intelligence, methods or motives of another person unless it is a factual response to a formal reference request
- provide or facilitate the use of computer hacking tools or virus toolkits.

5.2. Use of material for teaching/research purposes, which would otherwise be contrary to this policy, may be permissible at the discretion of the Headteacher.

5.3. Employees must not use the internet, email, telephone or any other form of electronic communication to send sensitive or subversive information, including:

- opinions that do not reflect the policies of Downs View (but see section 7.3 for Facilities Arrangements exception);
- information that could prejudice the security of Downs View/the council's assets or information;
- information that could damage Downs View/the council's reputation and standing in the community.

6. Data Protection

6.1. Downs View has nominated Data Protection Officers who are tasked with ensuring that we record, store and send data in compliance with the Data Protection Act 2018.

6.2. The Data Protection Act 2018 puts certain legal obligations on Downs View for the recording and storing of personal information. Any queries should be addressed to the Data Protection Officer.

6.3. Employees responsible for systems that record personal information must ensure that all such systems comply with the data protection principles

6.4. Any employee who develops a database, spreadsheet or other computer system that records personal information must ensure that the system complies with the Data Protection Act 2018.

7. Intellectual Property Rights

7.1. Material that is Copyrighted or Trademarked, or other proprietary material must not be copied, stored or transmitted without the express permission of the owner. Such action, whether knowing or inadvertent, may result in liability to the Downs View or the Council and/or the individual responsible.

7.2. Employees should be aware that, in general, the employer retains intellectual property rights to all material that is created by employees as part of their work. In certain circumstances the intellectual property rights may be shared, if an agreement to this effect is drawn up prior to such particular work being developed (See appendix 1).

8. System Security Policy

8.1. Downs View is responsible for establishing and enforcing a password policy for its use of ICT. Application system owners are responsible for establishing and enforcing a password policy on their systems based on the level of security required.

8.2. Passwords are assigned to individual users of ICT systems:

- to maintain the security of systems and the data that they contain;
- to ensure that all access and modification to the data can be traced back to an individual employee.

8.3. Ownership

- All systems have a “designated system owner”. This phrase is used to describe either the employee or the Council team that has the delegated responsibility for the maintenance and integrity of that system.
- Downs View Life Skills College applications are all owned by DVLSC.

8.4. Securing Passwords

- Employees must protect their passwords, as they will be held accountable for all activities undertaken under their usernames.
- Where written down they must be kept in a secure location such as a safe or cash box.
- Any password used by an employee must be provided, on request, to their Headteacher, Executive Director, Families Children and Learning, the Head of Personnel, or the Head of Audit & Risk Management or any nominated officer.
- Passwords should be chosen in a way that makes them difficult to guess.
- For each computer system that has its own acceptable password policy, this must be complied with by all users of that system.
- Groups of employees must not share the same password for their individual usernames unless there is a valid technical and operational reason. Such action defeats the objectives of secure and accountable access to data.

8.5. Staff Changes

- Line managers, or other nominated officers, should inform the Headteacher of all new employees so that the appropriate usernames and passwords can be created.
- When an employee leaves their job, whether leaving Downs View or not, the line manager, or other nominated officer, must inform the Headteacher immediately so that all usernames and passwords for that employee can be suspended as appropriate.

8.6. Access to Systems

- Employees must never attempt to gain unauthorised access to other computers, networks or information either within or external to Downs View/the council. This is an offence under the Computer Misuse Act.
- Employees must not use the username and password of another employee unless the access is in connection with a formal request for the provision of a password made by the Headteacher/council Head of ICT, Head of Personnel, or the B&H Head of Audit & Risk Management (or any of their nominated officers).

- Most computer systems will automatically suspend a username if repeated attempts are made to access it using an incorrect password. If this occurs then the employee to whom this username is assigned should contact the appropriate system manager to have the username unlocked.
- Employees must not give any person not employed by Downs View/the council access to any computer system without the written permission of the Headteacher/Executive Director or one of their nominated officers.
- Employees must not subvert any system that controls or monitors access to a computer system.

8.7. System Integrity

- Employees must not damage or compromise the integrity of any computer system.
- Any computer system, data or workstation taken off Downs View/Council premises must be protected with a security system specified by the Headteacher/Executive Director or one of their nominated officers.
- Employees must not alter any information held on any computer system for any reason other than the normal performance of their duties.
- Line Managers must ensure that where data backup or security procedures are delegated to them that these procedures are followed.

8.8. Encryption

- Files may be password protected where the application software has such a facility built in. Where files are password protected employees must make provision for line managers and/or colleagues to gain access to the file in their absence.
- Employees must not install or use any other encryption software without the written permission of the Headteacher/Executive Director or one of their nominated officers.

9. Email Policy

9.1. Downs View/the Council provides an email system for business use only. Employees should be aware of the importance of using email on a daily basis, using common courtesy in messages, performing regular housekeeping and discouraging excessive, inappropriate or wrongful use of the system.

9.2. Ownership and Privacy

- All emails originating, arriving, or in transit through the Downs View Outlook system is the property of the Downs View/the council.
- An employee may be granted access to use the Downs View email system at the discretion of management. Downs View reserves the right, in its sole discretion, to suspend or terminate the use by any person of email at any time, for good reason. In addition Downs View may take disciplinary action against any person who misuses email.

- The council strives to provide controls to safeguard information access to its email systems. The council reserves the right to monitor, access, review and disclose all messages without the additional consent being required from any employee, contractor, vendor or person who uses an email system belonging to the council. Surveillance may be undertaken for the purposes of audit, security or where there is reason to believe that a breach of this policy has occurred.
- Emails are not guaranteed to be private or to arrive at their destination either within a particular time, or at all.

9.3. Private Use

- Emails must not be used for private use other than where agreed as acceptable within this policy.
- If employees wish to send and receive private emails they should open a personal email account and access this service in their own time.

9.4. Acceptable Use

- Emails used to complete transactions, such as transfer of funds, must only be used in controlled environments that can ensure the authenticity of the originating persons.
- Employees should not send irrelevant or inappropriate email to mailing lists.
- Employees should be mindful of suspicious looking or “scam” emails.
- Employees must not use a third party email system in place of the Downs View’s system without the written approval of the Headteacher.
- Employees should report to their line manager, or such other appropriate officer, the receipt of any email that they consider to be offensive or that may be construed as bullying or harassment.
- Emails should be signed off with a signature that includes the first name, surname, job title, and the organisation.
- An employee receiving an email message in error must inform the sender immediately and delete the message from the system.
- Trade unions/professional organisations should use ICT in accordance with this policy.

9.5. House keeping

- As Outlook is a cloud-based system there is no longer the imperative for employees to keep the size of their mailbox low, however it is good house keeping to delete unnecessary emails regularly and file or archive those to be kept as appropriate.
- Employees should check their emails on a daily basis.
- Employees should set up an out of notifying other users sending messages when they are on leave for more than 2 days. The return message should give an alternative contact who can deal with work in their absence.

9.6. Good Practice Guidelines

- Email is intended for business use and whilst correspondence is generally briefer than other correspondence, try to use correct grammar and spelling making use of the spell checking facilities.
- Consider the correspondence to be permanent and do not assume that the email, when deleted, will be lost forever.
- Take care when communicating sensitive information.
- Take care when communicating with someone in another country as insensitive use could lead to litigation in that country.
- If training is required on the use of the email system please discuss this with your line manager.
- Do not communicate information via email that you would not be prepared to say to the recipient if you were talking face to face.
- Avoid using upper case in email as it is generally interpreted as shouting.
- Wherever possible, other people's comments or observations should be communicated verbatim by using the "threading" capability of email i.e. using Reply and Forward options so that the message history is retained (do not quote comments or observations from other people as a quote may be taken out of context).
- Care should be taken on the address as misaddressing is common.
- Clearly title messages so that the contents can be understood before the message is opened.
- Clearly mark a message "for information" if no action is required.
- Make it clear what action or response is required from each recipient.
- Do not copy or forward unnecessary messages to others.

9.7. Discussion Forums

- The council provides online discussion facilities for business usage. These facilities are maintained by the council and they may delete any message on any discussion forum at their discretion. School based moderators may delete messages in the particular discussion forums for which they hold responsibility.
- Employees should not post messages to discussion forums that are not relevant to the usage of that particular forum. Where doubt exists as to the usage of that particular forum then messages should not be posted.

10. Internet Policy

10.1. Downs View provides a secure, filtered and monitored internet feed, access to which may be granted to a member of staff at the discretion of their management.

10.2. Employees must not attempt to bypass either the security, filtering or monitoring services.

10.3. Employees must not access any unsuitable material that is not filtered.

10.4. Downs View/the Council reserves the right to monitor, access and review an individual's use of the internet without the additional consent being required from any employee. Surveillance may be undertaken for the purposes of audit, security or where there is reason to believe this policy has been breached.

10.5. An individual may request the private use of the internet under the following circumstances:

- that it is approved in advance by the employee's line manager including the length of time that it may be used privately;
- that it only occurs in the individual's own time (outside of contractual hours);
- that it complies with this policy on the use of the internet.

10.6. Employees must not download or install any programs without the permission of the Headteacher or a nominated officer.

11. Workstation Policy

11.1. Workstations are provided for business use and must not be used for any other purpose other than where agreed as acceptable within this policy.

11.2. All programs stored on a Downs View/council owned computer are the property of the Downs View/the council and not individual employees.

11.3. An employee may be granted access to use a workstation at the discretion of management. Downs View/the council reserves the right, in its sole discretion, to suspend or terminate the use by any person of any or all workstations, at any time. In addition Downs View may take disciplinary action against any person who misuses workstations or systems accessible through it.

11.4. Downs View/the council reserves the right to monitor, access and review an individual's use of workstations without the additional consent being required from any employee. Surveillance may be undertaken for the purposes of audit, security or where there is reason to believe this policy has been breached.

11.5. Every workstation has a designated person responsible for its use, for the software resident in the machine and for compliance of this policy. This person will be one of the following:

- the occupant of the desk on which the machine resides;
- the manager of an area where workstations are a shared resource for a group of users;
- a user allocated a portable workstation on a temporary or permanent basis.

11.6. The Headteacher or the line manager must retrieve all equipment from employees, contractors and temporary staff leaving their employment.

11.7. Workstations must be used only for Downs View/council business, unless express permission has been obtained from the line manager. Any private use must be undertaken outside of work hours and must not include:

- processing relating to commercial activities;
- importing or downloading of documents, data or software from other devices or sites;
- any activities that could potentially reduce the security of Downs View systems and data;
- creation of private intellectual property;
- saving any data to a network drive.

11.8. The following procedures apply ICT equipment is used off site:

- the individual must seek authorisation from their line manager;
- the employee and their line manager must sign a document stating the item of equipment, serial number or other relevant identification, the date that the equipment was taken off premises and the duration that it will be off site;
- the employee and their line manager must sign a document stating the date that an item of equipment is returned to the premises;
- the employee accepts responsibility for the equipment once it has been signed for;
- the Headteacher must be informed on the first occasion that an item of hardware is used off site and the documents referred to above must be made available for their inspection as required;
- Downs View is responsible for securing appropriate insurance for all equipment used off-site.

11.9. The software used by Downs View is very tightly controlled. The following restrictions apply to all software:

- all software installed must be properly licensed; the use of all software must comply with the conditions of the relevant licence agreement;
- all software installed must be relevant to the work of the the team or department in which it is based;
- any installation of software must only be done with the permission of the Headteacher (or nominated representative);
- free, public domain or shareware software is subject to the same restrictions on use as all other software and must only be installed in compliance with this policy;
- employees must not attempt to circumvent any security system installed on a workstation by management, this includes, but is not limited to, remote control software, automatic control software, lockdown software and antivirus software.

12. Telephones Policy

12.1. The telephone are designed for business use only. Personal use is only permitted in the following circumstances:

- authorisation has been sought from the employee's line manager, and the call is urgent and could not wait until an appropriate work break;
- the call is connected with the employee having to work later than expected;
- the call is a brief internal call;
- the employee reimburses the cost of the call, other than calls in connection with the employee working late.

12.2. Employees must not use Downs View's telephones or their own personal mobile phones to receive private calls whilst working unless the call is urgent.

12.3. Downs View reserves the right, in its sole discretion, to suspend or terminate any persons use of any telephone at any time. In addition Downs View may take disciplinary action against any person who misuses the telephones.

12.4. Telephone lines must not be connected, to any equipment without the permission of the Headteacher or one of their nominated officers.

Appendix 1 – Intellectual Property Rights agreement

(See Section 7 of The Use of ICT Policy)

Parties to the agreement:

N.B. Copyright resides with the employer

Name of staff member: …….

Name of Employer or Employer's representative (normally the Headteacher):

…….

School name: …….

2. Brief summary of the development project

We agree to share the proceeds of any profit made from the above project on the basis of 30% to the employee and 70% to the employer basis. (The employee is requested to seek their own legal advice if they have any concerns).

3. Signatures of the Parties:

Employee: …….. Date:……..

Employer: …….. Date:…….