Black Sluice Internal Drainage Board
Policy No: 43
Policy: Electronic Information and Communication Systems

Review	Audit & Risk Committee on 26th April 2017
Board Approved	14th June 2017
Reviewed	Within 5 years

INTRODUCTION

The Board's electronic communications systems and equipment are intended to promote effective communication and working practices within the Board, and are critical to the success of our business. This policy outlines the standards which the Board requires users of these systems to observe, the circumstances in which the Board will monitor use of these systems and the action we will take in respect of breaches of these standards. The sections below deal mainly with the use (and misuse) of computer equipment, e-mail, internet connection, telephones, and voicemail, but this policy applies equally to use of fax machines, copiers, scanners, CCTV, and electronic key fobs and cards. Workers are expected to have regard to this policy at all times to protect its electronic communications systems from unauthorised access and harm.

Breach of this policy may be dealt with under the disciplinary procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

POLICY

1. LEGISLATIVE FRAMEWORK

The use by workers and monitoring by us of our electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 1998 together with the Employment Practices Data Protection Code, issued by the Information Commissioner. We are also required to comply with the Regulation of Investigatory Powers Act 2016, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into United Kingdom law by the Human Rights Act 1998.

2. PERSONNEL RESPONSIBLE FOR IMPLEMENTATION OF POLICY

2.1 The Board has overall responsibility for this policy. Responsibility for monitoring and reviewing the operation of the policy and any recommendations for change to minimise risks to our operations also lies with the Finance Manager. The Finance Manager will deal with requests for permission or assistance under any provisions of this policy, subject to their primary and priority tasks of maintaining our core systems, and may specify certain standards of equipment or procedures to ensure security and compatibility.

2.2 Managers have a specific responsibility to operate within the boundaries of this policy, to facilitate its operation by ensuring that workers understand the standards of behaviour expected of them and to identify and act upon behaviour falling below these standards.

2.3 All workers are responsible for the success of this policy and should ensure that they take the time to read and understand it, and to disclose any misuse of the Board's electronic communications systems of which they become aware to the Chief Executive. Questions regarding the content or application of this policy should also be directed to the Finance Manager.

3. WHO IS COVERED BY THE POLICY

This policy covers all individuals at all levels and grades, including senior managers, officers, directors, employees, contractors, trainees, homeworkers, part-time and fixed-term employees, and agency staff (collectively known as workers in this policy), and also third parties who have access to the Board's electronic communication systems.

4. EQUIPMENT SECURITY AND PASSWORDS

4.1 Workers are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy. If given access to the e-mail system or to the internet, workers are responsible for the security of their terminals and, if leaving a terminal unattended or on leaving the office, should ensure that they lock the computer to prevent unauthorised users accessing the system in their absence. Workers without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the Finance Manager.

4.2 Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Finance Manager. For the avoidance of doubt, on the termination of employment (for any reason) workers must provide details of their passwords to the Board.

4.3 Workers who have been issued with a laptop, tablet or mobile phone must ensure that it is kept secure at all times, especially when travelling. Passwords or biometrics must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Workers should also observe basic safety rules when using such equipment, such as not using or displaying it obviously in isolated or dangerous areas. Workers should not use equipment on public transport or in other public areas where documents can be read by third parties.

5. SYSTEMS AND DATA SECURITY

5.1 Workers should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk.

5.2 Workers should not download or install software from external sources without authorisation from the Finance Manager. This includes programs, instant messaging programs, screensavers, photos, video clips and music files. Files and data should

always be virus-checked before they are downloaded. If in doubt, workers should seek advice from the Finance Manager.

5.3 No device or equipment should be attached to our systems without the prior approval of the Finance Manager. This includes any USB flash drive, MP3 or similar device, PDA or telephone. It also includes use of the USB port, infra-red connection port or any other port.

5.4 We monitor all e-mails passing through our system for viruses. Workers should exercise caution when opening e-mails from unknown external sources or where, for any reason, an e-mail appears suspicious (for example, if its name ends in .exe or .zip). The Finance Manager should be informed immediately if a suspected virus is received. We reserve the right to block access to attachments to e-mails for the purpose of effective use of the system and for compliance with this policy. We also reserve the right not to transmit any e-mail message.

5.5 Workers should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised.

5.6 Workers using laptops or wi-fi enabled equipment must be particularly vigilant about its use outside the office and take any precautions required by the Finance Manager from time to time against importing viruses or compromising the security of the system. The system contains information which is confidential to the Board´s business and/or which is subject to data protection legislation. Such information must be treated with extreme care.

6. E-MAIL ETIQUETTE AND CONTENT

6.1 E-mail is a vital business tool but an informal means of communication and should be used with great care and discipline. Workers should always consider if e-mail is the appropriate medium for a particular communication. Messages sent on the e-mail system should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals.

6.2 Workers should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling and use an out of office response when away from the office for more than a day. Workers should not expect colleagues to read or reply to e-mails sent or received out of office working hours.

6.3 Workers should not send abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded and should be reported to the Finance Manager. If a recipient asks you to stop sending them personal messages, then always stop immediately. Where appropriate, the sender of the e-mail should be referred to this policy and asked to stop sending such material. If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via e-mail, you should inform the Finance Manager who will usually seek to resolve the matter informally.

6.4 Workers should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal or Board liability in the same way as the contents of letters or faxes. For example, in connection with claims of discrimination, harassment, defamation, breach of confidentiality or breach of contract. Workers should assume that

e-mail messages may be read by others and not include in them anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain. The Board's standard disclaimer should always be used.

6.5 E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user´s inbox or archives does not mean that an e-mail is obliterated and all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

6.6 In general, workers should not:

(a) send or forward private e-mails at work which they would not want a third party to read;

(b) send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the Board;

(c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;

(d) sell or advertise using the systems or broadcast messages about lost property, sponsorship or charitable appeals;

(e) agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter;

(f) download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;

(g) send messages from another worker's computer or under an assumed name unless specifically authorised;

(h) send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.

6.7 Workers who receive an e-mail which has been wrongly delivered should return it to the sender of the message. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or used in any way.

7. USE OF THE WEB

7.1 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in paragraph 8.2, such a marker could be a source of embarrassment to the Board, especially if a worker has accessed, downloaded, stored or forwarded inappropriate material from the website. Workers may even be committing a criminal offence if, for example, the material is pornographic in nature (see section on Inappropriate Use of Equipment and Systems at paragraph 10).

7.2 Workers should not therefore access from the Board's system any web page or any files (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK, it may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person within the Board (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that the Board's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

7.3 Workers should not under any circumstances use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog, even in their own time.

7.4 Remember also that text, music and other content on the internet are copyright works. Workers should not download or e-mail such content to others unless certain that the owner of such works allows this.

8. PERSONAL USE OF SYSTEMS

8.1 The Board permits the incidental use of its internet, e-mail and telephone systems to send personal e-mail, browse the web and make personal telephone calls subject to certain conditions set out below. Our policy on personal use is a privilege and not a right. The policy is dependent upon it not being abused or overused and we reserve the right to withdraw our permission or amend the scope of this policy at any time.

8.2 The following conditions must be met for personal use to continue:

(a) use must be minimal and take place substantially out of normal working hours (that is, during a worker's usual lunch hour, before 7 am or after 5:15 pm);

(b) use must not interfere with business or office commitments;

(c) use must not commit the Board to any marginal costs; and

(d) use must comply with the Board's policies and procedures.

8.3 Workers should be aware that any personal use of the systems may also be monitored (see paragraph 9) and, where breaches of this policy are found, action may be taken under the disciplinary procedure (Paragraph 10). The Board reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers that personal use is excessive.

9. MONITORING OF USE OF SYSTEMS

9.1 The Board's systems provide the capability to monitor telephone, email voicemail, web and other communications traffic. Monitoring will only be carried out to the extent permitted or required by law and as necessary and justifiable for business purposes.

9.2 The Board reserves the right to monitor and keep records of use of the Board's IT system and email and internet access for a number of reasons relevant to its business including but not limited to:

(a) ensuring compliance with this policy;

(b) training and monitoring standards of service;

(c) ascertaining whether internal or external communications are relevant to the Board's business;

(d) preventing, investigating or detecting unauthorised use of the Board's IT system or criminal activities; and

(e) maintaining the effective operation of the Board's IT system.

9.3 The Board has a legitimate interest in protecting its business reputation and communication systems, limiting its exposure to legal liability and ensuring that workers conduct themselves and perform their work to the level expected of them.

10. INAPPROPRIATE USE OF EQUIPMENT AND SYSTEMS

10.1 Access is granted to the web, telephones and to other electronic systems, for legitimate business purposes only. Incidental personal use is permissible provided it is in full compliance with the Board´s rules, policies and procedures. See paragraph 8 on Personal Use of Systems.

10.2 Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with our disciplinary procedure. Misuse of the internet can, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

(a) pornographic material (that is, writings, pictures, films, video clips of a sexually explicit nature); or

(b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to the Board or to its clients; or

(c) a false and defamatory statement about any person or organisation; or

(d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others; or

(e) confidential information about the Board and any of its staff or clients; or

(f) any other statement which is likely to create any liability (whether criminal or civil, and whether for you or the Board; or

(g) material in breach of copyright; or

(h) online gambling; or

(i) chain letters.

Any such action will be treated very seriously and is likely to result in summary dismissal. Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our disciplinary procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the disciplinary procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

11. MONITORING OF POLICY

11.1 This policy reflects the law and the Board's practice as at 1st April 2017. The Chief Executive, in conjunction with the Board, shall be responsible for reviewing this policy from a legislative and operational perspective at least 5 yearly.

11.2 Staff are invited to comment on this policy and suggest ways in which it might be improved by contacting the Chief Executive.