I.T. SECURITY, ACCEPTABLE-USE AND PASSWORDS POLICY

IT SECURITY, ACCEPTABLE-USE AND PASSWORDS POLICY

1 ABOUT THIS POLICY

1.1 Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This Policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take in respect of breaches of these standards.

1.2 This Policy covers all board and committee members, officers, consultants, contractors, paid employees, volunteers, casual workers, members and anyone who has access to our IT and communication systems. All expressions such as “County business” or “County equipment” are to be read as including business or personal equipment, etc., unless the context clearly excludes them.

1.3 Misuse of IT and communications systems can damage the MCRFU and our reputation, as well as causing harm and distress to any affected individuals. Extremely large fines can be imposed on the MCRFU. Breach of this Policy on the part of employees may be dealt with as a disciplinary matter and, in serious cases, may be treated as gross misconduct leading to summary dismissal or removal from your post.

1.4 This policy does not form part of any contract between you and the MCRFU and we may amend it at any time.

2 PERSONNEL RESPONSIBLE FOR THE POLICY

2.1 The MCRFU Board members have overall responsibility for the effective operation of this Policy and for ensuring compliance with the relevant statutory framework. Day-to-day responsibility for operating the Policy and ensuring its maintenance and review has been delegated to the MCRFU Data Protection Officer, working with the MCRFU Chairman.

2.2 The Data Protection Officer reports directly to the Board. He/she is responsible for advising on and promoting compliance with our legal obligations and is obliged to report any breaches to the Information Commissioner. Issuing compliancy requirements to members, staff and volunteers, including matters relating to IT security, is part of his/her role.

2.3 All individuals and volunteers who work for the MCRFU have a specific responsibility to ensure the fair application of this Policy, and all individuals who work or volunteers for, or are members of the MCRFU, are responsible for supporting colleagues and ensuring its success.

2.3 The Data Protection Officer, advised by our IT Support providers, will deal with requests for permission or assistance under any provisions of this Policy, and may specify certain standards of equipment or procedures to ensure security and compatibility.

3 EQUIPMENT SECURITY

3.1 You are responsible for the security of the equipment allocated to or used by you, and must not allow it to be used by anyone other than in accordance with this Policy. "Security" covers both the physical control of the equipment against damage, loss or theft, and the prevention of unauthorised use whether by a "present user" or non-present hacker

3.2 You are responsible for the security of any computer device used by you. All devices should be completely shut-down at the end of the day's work. You should configure "sleep" settings so that logging-in is required if the device has been unused for more than five minutes. You should in any event lock up (Windows flag + L) off when leaving it unattended for more than a minute, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access our network must not be allowed to use our devices, unless logged in as an identified Guest/Visitor with restricted access rights.

3.3 Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting IT Support.

3.4 If using or transporting our IT equipment outside the workplace, as a minimum the following precautions must be observed:

3.4.1 Equipment must be stored in a secure place, not left in a car overnight, and if it has to be left in a car temporarily, it must be placed out of sight

3.4.2 Internet access must not be gained via insecure wi-fi where no password has to be entered. Use of semi-public Wi-Fi in hotels, conference centres or clubs etc, where many people will have the password, must be minimised and devices should not be left connected any longer than absolutely necessary.

3.4.3 Firewalls and anti-virus programs installed by the MCRFU should not be disabled or reconfigured.

Users must take such further precautions as we may require from time to time against importing viruses or compromising system security.

3.5 For those authorised to use their own devices on MCRFU business, please read the Bring Your Own Device ("BYOD") Policy

3.6 Smartphones used for MCRFU business, or on which MCRFU e-mails can be read, must have strong log-ins (a six-digit code is stronger than a nine-point swipe: a fingerprint is best of all, where available) and a short lock-up time – no more than three minutes. It is recommended that they should be equipped with remote-locking and tracing apps in event of theft or loss.

3.7 Where there are multiple users of a single computer, each must have a separate login identity. There must not be a single "Club" identity. Folder access permissions should be allocated to each appropriately.

4 SYSTEMS AND DATA SECURITY

4.1 You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

4.2 You must not download or install software from external sources onto MCRFU equipment without authorisation from the County Secretary. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked before / as they are downloaded. Be aware of the risk of virus infection if poorly-secured personal devices are plugged in to MCRFU equipment - This includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, Bluetooth connection or in any other way.

4.3 Although we check all emails passing through the MCRFU systems for viruses you must not rely on this technology. Always exercise the upmost vigilance when opening emails and email attachments on any device. If in any doubt inform your IT Support provider for a second opinion. You should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious (for example, if it contains a file whose name ends in .exe) (see Appendix 2). Inform your IT Support provider immediately if you suspect your computer may have a virus or if you have opened any suspicious email attachments or clicked on any suspicious links. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

4.4 You must not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

4.5 See Appendix One for our **Passwords Policy**

5 EMAIL

The email rules below apply to anyone who has a MidlesexRugby.com email address be they board member, volunteers or staff.

5.1 Although email is a vital business tool, you should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals.

5.2 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails. Anyone who feels that they are being or have been harassed or bullied, or is offended by material received from a colleague via email, should inform the county secretary.

5.3 You should take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that you have no control over where your email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties, or found its way into the public domain.

5.4 Email messages are required to 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 email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software. For sensitive material, remember that e-mail is "no more secure than a seaside postcard".

5.5 In general, you should not:

5.5.1 send, forward or read private emails from your MCRFU email account which you would not want a third party (i.e. someone not known to you) to read;

5.5.2 send or forward chain mail, junk mail, cartoons, jokes or gossip;

5.5.3 contribute to system congestion or filling your MCRFU inbox by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list;

5.5.4 sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;

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

5.5.6 download or email text, music or any other content on the internet which is subject to copyright protection, unless it is clear that the owner of such works allows this;

5.5.7 send messages from another person's email address (unless authorised) or under an assumed name

5.5.8 send or forward a message to multiple recipients unless you use the "BCC" field so that the recipients cannot see each other's e-mail addresses (this does not apply to a small group of users who already know each other's addresses).

5.6 You should keep you MCRFU mail box in order. If your inbox fills up please clear some space by delete emails no longer required. You can request that your inbox is extended.

5.7 If you receive an email in error you should inform the sender. If you have sent an email in error which might cause harm or embarrassment, contact the county secretary immediately.

5.8 We are trying to move away from the use of personal email accounts, particularly by county volunteers, to send or receive email for the purposes of our business. If not already provided, ask if an email account can be provided for you.

5.9 See Appendix Two for guidance on how to recognise fake or spam e-mails and prevent your computer getting infected.

6 USING THE INTERNET

6.1 Internet access while in the MCRFU offices is provided primarily for business purposes. Occasional personal use may be permitted as set out in paragraph 7.

6.2 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 9.1, such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

6.3 You should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content which is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our 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. Remember this is how criminals gain access to your or our systems.

6.4 Except as authorised in the proper performance of your duties, you should not under any circumstances use our systems, email or MCRFU social media platforms 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 or wiki.

6.5 If you accidentally visit a website, or download content, of the type mentioned in 6.3, it should be reported to the County Secretary so that it can be safely removed and a virus check carried out.

7 PERSONAL USE OF OUR SYSTEMS

7.1 We permit the incidental use of our internet, email and telephone systems to send personal email, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

7.2 Personal use must meet the following conditions:

7.2.1 use must be minimal and take place substantially out of normal working;

7.2.2 personal emails should be labelled “personal” in the subject header;

7.2.3 use must not interfere with business or office commitments;

7.2.4 use must not commit us to any marginal costs; and

7.2.5 use must comply with this Policy (see in particular paragraph 5 and paragraph 6) and our other policies including our Data Protection Policy and Privacy Policy for Websites.

7.3 You should be aware that personal use of our systems, email and social media may be monitored (see paragraph 8) and, where breaches of this Policy are found against an employee, action may be taken under Disciplinary Procedure (see paragraph 9). We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

7.4 See Appendix Three for our Social Media Policy

8 MONITORING

8.1 Our systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

8.2 In certain locations, CCTV systems monitor the exterior of the building 24 hours a day. This data is recorded, is accessible by the security company providing the service, and may be made available to the police. Such locations should be identified by a public and prominent notice. This applies also to any churches filming their services for “live streaming” or later viewing.

8.3 We reserve the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

8.3.1 to monitor whether use of the email system or the internet is legitimate and in accordance with this Policy;

8.3.2 to find lost messages or to retrieve messages lost due to computer failure;

8.3.3 to assist in the investigation of alleged wrongdoing; and

8.3.4 to comply with any legal obligation.

9 PROHIBITED USE OF OUR SYSTEMS

9.1 Misuse or excessive personal use of our telephone or email system or inappropriate internet use will be dealt with as a disciplinary matter. Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse our systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):

9.1.1 pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

9.1.2 offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our parishioners;

9.1.3 a false and defamatory statement about any person or organisation;

9.1.4 material which is discriminatory, offensive, derogatory or may cause embarrassment to others;

9.1.5 confidential information about us, our work, or any of our workers, or volunteers (except as authorised in the proper performance of your duties);

9.1.6 any other statement which is likely to create any criminal or civil liability (for you or us); and/or

9.1.7 music or video files or other material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal or removal from your post.

9.2 Where evidence of misuse is found against an employee or volunteer, we may undertake a more detailed investigation, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses involved in the investigation process. If necessary, such information may be handed to the police in connection with a criminal investigation.

APPENDIX ONE

PASSWORDS POLICY

Passwords are an integral aspect of our IT Security Policy. Passwords are the front line of protection for user and email accounts. A poorly chosen password may result in the compromise of critical resources. As such, all staff, members, volunteers and external third parties with access to our systems are responsible for taking the appropriate steps to select and secure their passwords.

All passwords must conform to the following guidelines:

1. It is recognised that it is impractical to change passwords frequently. Nonetheless, it is Good Practice to change your key passwords every so often – certainly every year.

2. Passwords must not be included in email messages or other forms of electronic communication.

3. Passwords must be at least 8 characters in length. Passwords or pass phrases should be as long as can be remembered or practicably typed. Length is a crucial factor in password strength

4. Strong passwords must be used (see guidance below).

5. If a password is not easy to memorise, a written record may need to be kept but.... Do not write down passwords anywhere obvious, such as on a Post-It stuck on the edge of your monitor, or keeping them in a text file on your PC with an obvious name like “passwords.doc”.

6. Do not store passwords on-line without encryption.

7. Do not use the same password for MCRFU accounts as for other non-MCRFU access (e.g., personal on-line banking, personal email etc.).

8. Do not share MCRFU passwords with anyone. If Para 3.7 is complied with, there should be no need to share passwords with other users of e.g. the office computer. There should be a record of who knows the password. All passwords are to be treated as sensitive, confidential information. This is without prejudice to the requirement to lodge sealed copies of all passwords used on your computer(s) with the county secretary, so that your devices may be accessed in the event of your death or incapacity.

9. Don't talk about a password in front of others or hint at the format of a password (e.g., "my family name").

10. Disable the "Remember Password" features of some internet browsers such as Internet Explorer/Edge, Firefox, and other applications where this might be a feature.

12. If an account or password is suspected to have been compromised, report the incident to the County Secretary and change all passwords *immediately*.

Guidance on selecting strong passwords

It is important that everyone is aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

1. The password can be found in a dictionary (English or foreign).

2. The password is a common usage word such as: names of people, pets, companies or fictional characters; birthdays and other personal information such as addresses and phone numbers; computer related terms (e.g. ‘software’).

3. The password can be guessed-at by reference to personal details disclosed on Facebook or social media, such as birthdays, children’s or pet’s names, etc.

4. Simple word, number or keystroke patterns like 123456, aaabbb, qwerty, zyxwvuts, 123321.

5. The password is short. A four- or six-digit password is barely worth having.

Current IT-security-industry advice is towards **"pass phrases",** which are easy for you to remember and uncrackable by brute-force computer programs.

They consist of three or four short words, separated by spaces, which would never be found close together in a dictionary or normal writing – in other words there is a randomness about them – but they are easily memorable by you, either visually as a mental "cartoon", or because they are striking, or are meaningful to you.

An example (do not use this) would be "fish rock cowboy", memorised as a cartoon of a fish in a bowl, an aquarium rock, and a toy cowboy (like Woody in Toy Story) sitting on it. According to the website howsecureismypassword.net, this 16-character pass-phrase would take 224 million years to crack. Yet you have probably memorised it already.

The more traditional, but less easily-memorable, **strong password**s have the following characteristics:

1. Contain both upper- and lower-case letters (e.g., a-z, A-Z).

2. Have digits and punctuation marks or symbols as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

3. Are at least eight alphanumeric characters long. (The longer, the harder.)

4. Are not a word in any language, slang, dialect, jargon, etc.

5. Are not based on personal information, names of family, etc.

APPPENDIX TWO

Recognising fake e-mails (Phishing)

Fake e-mails are sent in large numbers for different purposes

- To try and get you to click on a link in the message, or open an attachment, which could infect your computer with a virus or have it taken over as a "slave" or "bot" device. Attached or embedded files with a filename ending in "exe" are to be treated with *particular* caution.
- To collect names from your Contacts list to sell to spammers – or just to build up a list of valid e-mail addresses where messages have been opened or replied-to.
- To attempt to obtain money or Bank details from you

The first General Principle is to be *very suspicious* of anything that looks a little out of the ordinary – even if it seems to come from someone you know (their computer may have been hacked-into)

The second General Principle is that if any offer or inducement looks too good to be true, it certainly is.

Common types of fake e-mails are:

- Messages offering you untold wealth if you will help someone move funds out of their country to the UK. Or telling you, you have won a prize.
- Messages seemingly from people you know saying that they have been robbed on holiday and asking for a brief loan
- Messages looking as if they are from your Bank asking you to confirm your details or click on a link.
- Unexpected messages looking as if they are from a company asking you to pay an invoice.
- Unexpected messages looking as if they are from the HMRC, DVLA, Police, NHS, etc. as an enticement saying that you have a rebate, your license has been cloned, your bank account hacked, you should contact them regarding a medical condition. Messages to pray on your fears or desires.
- Fake chasing messages from a supposed supplier threatening legal action
- Messages from a company claiming to be from domain-registration telling you that you must pay to keep your website up.
- Short messages from people you know inviting you to look at a photo or follow a link. Unless you're sure it's really from your acquaintance, check with them before opening it.

Some fraudsters have proved quite skillful in dressing up messages in "rugby language" if their target audience is people named in RFU contacts-lists.

There is a less dangerous type of message which is like a Chain Letter, predicting Bad Luck if it is not forwarded to all your friends, or warning you of some scam or threat. Do not forward these. Delete them. They just clog up the system. Their originators get a kick out of seeing how far round the world they can go.

There are several reputable Scam Warning websites which will tell you if a message is a known scam or fake.

Enable your Preview Pane, and Never, Ever, open a message, or click on a link in it, if you are the least bit uneasy about it.

APPENDIX THREE

SOCIAL MEDIA

This policy deals with the use of all forms of social media, including Facebook; LinkedIn; Twitter; Instagram; YouTube; all other social networking sites and all other internet postings, including blogs. It applies to the use of social media for both business and personal purposes, whether or not during office hours or otherwise. This policy applies regardless of whether or not the social media is accessed using our IT facilities and equipment, or equipment belonging to you. To be quite clear, this also applies to what you do at home and in your own time.

You may be required to remove immediately any internet postings and social media communications which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action including dismissal.

You must not post statements that could be construed as being damaging or detrimental to our ethos or reputation, or communicate disparaging or defamatory statements, using social media or otherwise, about:

- The MCRFU or RFU
- our employees
- our 'members' or member clubs
- our suppliers; or
- our agents and contractors

You are personally responsible for what you communicate via social media. Remember that what you publish might be read by an audience wider than you intended. You should ensure that any social media communication is communicated on your own behalf and does not appear to be linked with us in any way.

If you disclose via a social media communication that you are an employee or volunteer of the MCRFU, you must state that any views are entirely your own and do not represent our views. You must not post comments about sensitive or confidential business-related topics.

Breach of this policy by an employee may result in disciplinary action being taken against them including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach.

If you are suspected of committing a breach of this policy you will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details. If you become aware of a breach of this policy you must notify the county secretary.

This is not an attempt to limit freedom of speech or the right to criticise; but we expect certain standards and loyalty from our employees and volunteers, and breach of this policy will be regarded as a disciplinary matter for employees, and may lead to removal from roles for volunteers.

Document Approval History

Date	Version	Document Approver	Comment
1/07/2020	Version 1.2	County Secretary	Policy redrafted in June 2020