Procedure: General Data Protection Regulation & IT Policy.

1. SUMMARY

1.1. The purpose of this procedure is to define the requirements for providing an infrastructure capable of meeting the operational, training and general administration requirements of WINNS

1.2. The policy describes in detail the method by which the strategy is implemented.

1.3. The Operations Director is responsible for implementation and management of this procedure.

2. REVISION AND APPROVAL

Rev.	Date	Nature of Changes	Approved By
1	27/02/2018	Original issue.	C Stebbing
2	08.03.2018	Updated GDPR	C Stebbing

3. PROCEDURE

STATEMENT OF INTENT

The General Data Protection Regulation (GDPR) is designed to protect the privacy of individuals. It requires that any personal information about an individual is processed securely and confidentially. This includes both staff and children. How WINNS obtains, shares and uses information is critical, as personal data is sensitive and private. Everyone has the right to know how the information about them is used. The General Data Protection Regulation requires WINNS to strike the right balance in processing personal information so that an individual's privacy is protected. Applying the principles to all information held by WINNS will typically achieve this balance and help to comply with the legislation

We will respect the privacy of staff. We aim to ensure that all staff can share their information in the confidence that it will only be used to enhance the welfare of themselves. There are record keeping systems in place that meet legal requirements; means of storing and sharing that information take place within the framework of the General Data Protection Regulation and the Human Rights Act.

4. GENERAL DATA PROTECTION REGULATION PRINCIPLES

To comply with the act, WINNS must observe the eight 'General Data Protection Regulation principles', ensuring that:

4.1. Personal data shall be processed fairly and lawfully

4.2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

4.3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4.4. Personal data shall be accurate and, where necessary, kept up to date.

4.5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

4.6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

4.7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

4.8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In practice, it means that WINNS must:

4.9. have legitimate grounds for collecting and using the personal data;

4.10. not use the data in ways that have unjustified adverse effects on the individuals concerned;

4.11. be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;

4.12. handle people's personal data only in ways they would reasonably expect; and

4.13. make sure they do not do anything unlawful with the data

Personal data is information that relates to an identifiable living individual that is processed as data. Processing amounts to collecting, using, disclosing, retaining or disposing of information. The General Data Protection Regulation principles apply to all information held electronically or in structured paper files.

The principles also extend to personnel records – the names of staff and next of kin, dates of birth, addresses, national insurance numbers, education history, medical information, criminal records and staff development reviews.

Sensitive personal data is information that relates to

- race and ethnicity,
- political opinions,
- religious beliefs,
- membership of trade unions,
- physical and mental health,
- sexuality
- criminal offences

Sensitive personal data is given greater legal protection as individuals would expect certain information to be treated as private or confidential – for example, a manager or staff member may have a WINNS Services e-mail account that is made publicly available on the website whereas their home e-mail account is private and confidential and should only be available to those to whom consent had been granted.

It is important to differentiate between personal information that individuals would expect to be treated as private or confidential (whether or not legally classified as sensitive personal data) and personal information you can make freely available. For example: WINNS manager's identity is personal information but everyone would expect it to be publicly available. However, WINNS manager's home phone number would usually be regarded as private information.

What must WINNS do?

4.14. We must notify the ICO (Information Commissioner's Office) that we are processing personal data.

4.15. We have a nominated individual, WINNS Operations Director, as the 'Data Protection Controller'.

4.16. WINNS has clear, practical policies and procedures on information governance for staff to follow, and needs to monitor their operation

4.17. These should include:

- Staff Code of Conduct
- Privacy notices for staff

Data Breaches – In the event of a personal data breach, the Data Protection Controller should be notified immediately and an investigation carried out.

5. INDIVIDUAL RIGHTS

The General Data Protection Regulation includes the following rights for individuals:

5.1. the right to be informed;

5.2. the right of access;

5.3. the right to rectification;

5.4. the right to erasure;

5.5. the right to restrict processing;

5.6. the right to data portability;

5.7. the right to object; and

5.8. the right not to be subject to automated decision-making including profiling.

The General Data Protection Regulation entitles an individual the right to request the personal information this is known as a Subject Access Request (SAR) and includes all and any information held by WINNS, not just that information held on central files or electronically, so it could also include correspondence or notes held by others in the management team.

5.9. SARs must be responded to within 1 month of receipt.

5.10. The SAR should be made in writing by the individual making the request.

5.11. WINNS can refuse or charge for requests that are manifestly unfounded or excessive

6. STAFF RESPONSIBILITIES

Staff need to know and understand:

6.1. How to manage, keep and dispose of data

6.2. When they are allowed to share information with others and how to make sure it is kept secure when shared.

7. INFORMATION AND IT EQUIPMENT ACCEPTABLE USAGE

Acceptable Usage covers the security and use of all WINNS Services information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This applies to all WINNS Services employees, contractors and agents (hereafter referred to as 'individuals').

This applies to all information, in whatever form, relating to WINNS Services business activities, and to all information handled by WINNS Services relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by WINNS Services or on its behalf.

8. COMPUTER ACCESS CONTROL – INDIVIDUAL'S RESPONSIBILITY

Access to the WINNS Services IT systems is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the WINNS Services IT systems.
All user must seal in an envelope their user name and password and hand it to the Operations Director for contingency planning and operations.

Individuals must not:

8.1. · Allow anyone else to use their user ID and password on any WINNS Services IT system

8.2. · Leave their user accounts logged in at an unattended and unlocked computer.

8.3. · Use someone else's user ID and password to access WINNS Services IT systems

8.4. · Leave their password unprotected (for example writing it down).

8.5. · Perform any unauthorised changes to WINNS Services IT systems or information

8.6. · Attempt to access data that they are not authorised to use or access.

8.7. · Exceed the limits of their authorisation or specific business need to interrogate the system or data.

8.8. · Connect any Non-WINNS Services authorised device to the WINNS Services network or IT systems

8.9. · Store WINNS data on any non-authorised WINNS Services equipment

8.10. · Give or transfer WINNS Services data or software to any person or organisation outside WINNS Services without the authority of WINNS Services Data Controller.

Managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

9. INTERNET AND EMAIL CONDITIONS OF USE

Use of WINNS Services internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to WINNS Services in any way, not in breach of any term and condition of employment and does not place the individual or WINNS Services in breach of statutory or other legal obligations.
All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

9.1. Use the internet or email for the purposes of harassment or abuse.

9.2. Use profanity, obscenities, or derogatory remarks in communications

9.3. Access, download, send or receive any data (including images), which WINNS Services considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.

9.4. Use the internet or email to make personal gains or conduct a personal business

9.5. Use the internet or email to gamble

9.6. Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.

9.7. Place any information on the Internet that relates to WINNS Services, alter any information about it, or express any opinion about WINNS Services, unless they are specifically authorised to do this.

9.8. Send unprotected sensitive or confidential information externally.

9.9. Make official commitments through the internet or email on behalf of WINNS Services unless authorised to do so.

9.10. Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.

9.11. In any way infringe any copyright, database rights, trademarks or other intellectual property.

9.12. Download any software from the internet without prior approval of from WINNS.

9.13. Connect WINNS Services devices to the internet using non-standard connections

10. CLEAR DESK AND CLEAR SCREEN POLICY

In order to reduce the risk of unauthorised access or loss of information, WINNS Services enforces a clear desk and screen policy as follows:

10.1. Personal or confidential business information must be protected using security features provided for example lockable filing cabinets and lockable draws.

10.2. Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.

10.3. Care must be taken to not leave confidential material on printers or photocopiers.

10.4. All business-related printed matter must be disposed of using confidential waste bins or shredders.

11. WORKING OFF-SITE

It is accepted that Laptops, iPads, iPad and mobile devices will be taken off-site. The following controls must be applied:

11.1. Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.

11.2. Laptops, iPads must be carried as hand luggage when travelling.

11.3. Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop. iPad encryption must be used.

11.4. Particular care should be taken with the use of mobile devices such as Laptops, iPads, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

12. MOBILE STORAGE DEVICES

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only WINNS Services authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

13. SOFTWARE

Employees must use only software that is authorised by WINNS Services on WINNS Services computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on WINNS Services computers must be approved and installed by WINNS Services.

Individuals must not:

13.1. Store personal files such as music, video, photographs or games on WINNS Services IT equipment

14. VIRUSES

The IT support has implemented centralised, automated virus detection and virus software updates within the WINNS Services. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

14.1. Remove or disable anti-virus software

14.2. Attempt to remove virus-infected files or clean up an infection, other than by the use of approved WINNS Services anti-virus software and procedures.

15. TELEPHONE (VOICE) EQUIPMENT CONDITIONS OF USE

Use of WINNS Services voice equipment is intended for business use. Individuals must not use WINNS Services voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

Individuals must not:

15.1. Use WINNS Services voice for conducting private business

15.2. Make hoax or threatening calls to internal or external destinations

15.3. Accept reverse charge calls from domestic or International operators, unless it is for

15.4. business use

16. ACTIONS UPON TERMINATION OF CONTRACT

All WINNS Services equipment and data, for example Laptops, iPads and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to WINNS Services at termination of contract.
All WINNS Services data or intellectual property developed or gained during the period of employment remains the property of WINNS Services and must not be retained beyond termination or reused for any other purpose.

17. MONITORING AND FILTERING

All data that is created and stored on WINNS Services computers is the property of WINNS Services and there is no official provision for individual data privacy, however wherever possible WINNS Services will avoid opening personal emails.
IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. WINNS Services has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.
Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the

Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000

It is your responsibility to report suspected breaches of security without delay to WINNS management team.

All breaches of information security will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with WINNS Services disciplinary procedures.

18. ACCESS TO STAFF PERSONAL DATA

18.1. Employees are allowed to have access to all personal data about them held on manual or computer records under the Data Protection Act (1998). The Act requires the organisation to action requests for access to personal data within one month.

18.2. Should an employee request access to their personal data, the request must be addressed in writing to the relevant line manager. The request will be judged in the light of the nature of the personal data and the frequency with which they are updated. The employee will be informed whether or not the request is to be granted. If it is, the information will be provided within one month of the date of the request.

18.3. In the event of a disagreement between an employee and the data controller regarding personal data, the matter should be taken up under the WINNS grievance procedure.

18.4. The right of employees to see information held about them is extended to information held in paper record-keeping systems as well as computerised systems.

18.5. There are some exemptions; for example, employees will not be able to see employment references about them supplied in confidence, nor will people involved in negotiations with the data controller be able to see information about the data controller's intentions in relation to those negotiations.

18.6. Employee data cannot be used for direct marketing (including fundraising) if the data subject objects. Approval to use employee data for marketing purposes must be sought from the Data Controller.

19. LEGAL FRAMEWORK

19.1. General Data Protection Regulation 2018 https://ico.org.uk/

19.2. Data Protection Act 1998

19.3. Computer Misuse Act 1990

19.4. Freedom of Information Act 2000

19.5. Human Rights Act 1999