WAKEFIELD INDEPENDENT SCHOOL

POLICY TITLE	**Data Protection and ICT Acceptable Use Policy**

Policy Area	General
Author	Senior Management
Relevant Statutory Regulations	ISSR Part 3, 9; Data Protection Act 1998
Senior Team Lead	Senior Management
Version	2018.2
Last Updated	September 2023
Review Date	As required

Data Protection and ICT acceptable use Policy

1 Aims

1.1 This purpose of this policy is to provide guidance to staff, council members and volunteers to the School and also contains The Schools acceptable ICT policy.

2 Introduction

2.1 The School Data Protection Officer is responsible for ensuring information security. This policy applies to all staff, volunteers and governors/trustees.

2.2 All members of staff must be inducted by the IT Manager before using the School's ICT systems. Non staff are allowed use of the School's wireless service for the purpose of domestic internet access only and must be issued with an account (or their device registered with the IT department)

3 Safeguarding and Prevent

3.1 This policy supports the aim of The School to prioritise safeguarding and to provide a safe learning and working environment for students and staff, in line with:

(a) The Education Act 2002 to promote and safeguard the welfare of children and vulnerable adults.

(b) Keeping Children Safe in Education 2023

(b) The Counter Terrorism and Security Act 2015 to help prevent people being drawn into terrorism.

3.2 Staff are responsible for the wellbeing of students and must ensure that students are not accessing inappropriate material for their age or communicating with extremist groups. Pupils who staff feel are showing interest in extremist, abusive or inappropriate material should report this to the safeguarding staff.

Further information can be found within The School's Safeguarding and ICT policies

4 Security and use of ICT systems

1. School computers

4.1 The following measures will be undertaken by the IT department to ensure that School computers are secure:

(a) All School computers will be protected by a firewall and antivirus software, all security updates and patches will be applied

(b) Regular backups will be taken and kept in a secure place

(c) Staff will only be allowed access to the information that they need to carry out their jobs.

(d) All data will be securely removed or destroyed from a School computer when it is decommissioned

(e) School laptops that are issued to members of staff and may contain School data will be encrypted

(f) Secure passwords policies will be enforced on staff and student accounts.

4.2 The contents of the School's IT resources and communications systems are the property of the School. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communication systems except under the conditions laid out in 4.3 and 4.4

4.3 Staff are permitted to use personal devices on the school network. Data transmitted to and from personal devices though the schools' internet will be kept private. Logs of user activity are recorded and will be kept private except under the conditions laid out in 4.5

4.4 Staff are permitted to use school telephones for emergencies only and call logs will be kept private.

4.5 A log of all users' activity on the School network will be held for a reasonable time period. This information will be kept private unless requested for an appropriate reason, examples might include but are not limited to:

(a) Establishing the existence of facts
(b) Ascertaining compliance with regulatory or self-regulatory procedures
(c) Monitoring standards which are achieved by persons using the school's computers, telephony (except for telephones provided in staff accommodation) or hosted communication platforms (such as email and intranet) in the course of their duties and for staff training purposes.
(d) Prevention or detection of crime
(e) To investigate or detect unauthorized use of the School's telecommunication system
(f) To ensure the effective operation of the system such as protecting against viruses, backing up and making routine interceptions such as forwarding e-mails to the correct destination
(g) For access to routine business communications, for instance checking voice mail and e-mail when staff are on holiday or on sick leave.

4.6 Staff must adhere to the following guidelines:

(a) All School passwords should be secure and never shared
(b) USB memory sticks or other removable media (including CDs or DVDs should never be used to carry School data unless they are encrypted. (The School could be fined £500,000 if, for example, a USB memory stick containing personal data is lost and not encrypted.)
(c) Only the minimum amount of data that is required to carry out your work should be copied to removable media such as USB memory sticks (encrypted)
(d) Staff computers should only be used by students under close supervision
(e) Never leave a laptop or digital device on show in a car or unattended in a public space
(f) Always make confidential phone calls in a private space and never in public (such as on a train)
(g) Avoid sending confidential information by fax or email (especially to external mail accounts). Data can be easily encrypted by simply applying a password to a Microsoft Word or Microsoft Excel file (the password should then be communicated separately with a verbal communication or via a text message)

(h) Paper records should be kept in accordance with your departments determined retention policy and should never be kept for longer than necessary (as detailed in Section 12)
(i) Paper documents containing personal or confidential information should be disposed of using the School's shredding service via the provided transit bags

2. Email and internet Use

4.7 The following procedures will be adhered to by all staff when using the School email system:-

(a) The use of a personal email account for School business is prohibited
(b) When sending email to multiple external recipients the bcc field should always be used
(c) The School email system should only be accessed from a secure private computer
(d) Appreciate that electronic mail is relatively insecure and consider security needs and confidentiality before transmission
(e) No one except the named individual should has access to their school email account, except during an identified period, such as during absence, when they will alert all people who use this account that it is being managed by someone else

4.8 Staff using the School's email or internet service must not:

(a) Create, transmit or cause to be transmitted material which is designed or likely to cause annoyance, inconvenience, needless anxiety or offence, and must not create, transmit or cause to be transmitted offensive obscene or indecent material

(b) Create, transmit or cause to be transmitted defamatory material

(c) Create, transmit or cause to be transmitted material such that the copyright of another person or party is infringed

(d) Transmit by e-mail any confidential information of the School otherwise than in the normal course of your duties

(e) Send any message internally or externally which is abusive, humiliating, hostile or intimidating

3. Cloud Storage

4.9 The following procedures will be adhered to by all staff when using Cloud based storage

(a) The use of personal cloud storage solutions (such as, but not limited to Dropbox, Google Drive and OneDrive) for storage of any School data is prohibited. (unless explicitly allowed by the IT Manager)

(b) Staff wishing to use cloud based storage must utilise the School's subscription to Microsoft OneDrive Professional.

(c) Any offline synchronization of the School's cloud storage (using for example the Microsoft OneDrive professional sync client) on mobile devices or personal devices that are not encrypted is prohibited.

4. Personal Devices

4.10 We recommend in the first instance that staff make use of the School's IT facility whenever possible and at all times minimize the amount of data that is held on personal devices.

4.11 When using a personal device to access/store School data or systems, the device must be secured with a strong password. (i.e. contain a mix of upper and lower case characters, numbers and punctuation and be at least 6 characters in length)

4.12 Personal devices should be configured to automatically lock after a short period of inactivity (5-15 minutes)

4.13 School files or data should never be stored on a shared device

4.14 Personal devices (and backup drives) used to store School data or files should be encrypted (for computers that cannot be easily encrypted we recommend the use of an encrypted USB memory stick). Please visit the IT department if you require advice on encrypting your device - most modern phones and computers now support this facility but it is often not turned on by default. Currently only Apple iPads and iPhones are encrypted by default

4.15 If a mobile or tablet device cannot be encrypted, the School will allow limited access to email via webmail or using the 'Microsoft OWA' app (if available)

4.16 Any device connected to the School's email system will be forced to enable a lock code and remote wipe facility (if compatible) - you agree to allow the School access to remotely wipe your device if we deem such an act necessary

4.17 You agree to keep any personal device that is used for School business fully updated with all operating system security patches and to use an antivirus/malware security program

4.18 Email and Intranet access is strictly prohibited on a shared computer unless the account/profile is secured to the individual member of staff

4.19 If your device has a remote locate and wipe facility you agree to enable this facility

5. Public Wi-fi and LANs

4.20 Any member of staff using a personal device for School business on a Public Wi-Fi connection will adhere to the following procedures

(a) You will only use a Public Wi-Fi connection from a trusted source (for example a Hotel service)

(b) Where applicable devices must have a firewall enabled and file sharing turned off.

(c) You will take extra care to verify that the sites you are visiting are genuine and secure.

(d) When using a laptop or desktop computer you default to using the School's remote desktop service whenever possible.

6. Removal of School Data from Personal Devices

4.21 If you believe that School data has been stored on a non-encrypted device the device should be securely wiped using a suitable software tool before disposal.

4.22 Upon termination of your employment contract you agree to securely delete any School data from your personal devices or memory sticks.

7. Storage and Use of Data within the School's Data Repositories

4.23 Staff will adhere to the following procedures when working with data held within the School's onsite and cloud based systems:

(a) All data (including email and calendars) will be secured so that only appropriate individuals will have access to it. (The IT department can assist with configuring sharing preferences with specific permissions)

(b) Data intended for staff will not be stored in areas used for student sharing

(c) All School devices or personal devices containing School information should be digitally locked when left unattended on the School's premises

5 Personal Data

8. Personal Data

5.1 Personal data covers both facts and opinions about an individual. It includes information necessary for employment such as the worker's name and address and details for payment of salary.

9. Processing of Personal Data

5.2 A worker's consent may be required for the processing of personal data unless processing is necessary for the performance of the contract of employment or by law. Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential and will often only be disclosed to third parties with the consent of the worker. Data may be disclosed to third parties without consent in certain circumstances such as but not limited to the following examples:

(a) A parent makes a complaint about a member of staff

(b) Information in staff witness statements may be disclosed for purposes of addressing bullying or harassment allegations

(c) Where allegations have been made against a member of staff which are reported to staff/social services

(d) Where it will ensure the safety of other members of the Wakefield Independent School community including pupils, staff and members of council

(e) If the School is required to do so by the law

10. Sensitive Personal Data

5.3 The School may, from time to time, be required to process sensitive personal data regarding a worker. Sensitive personal data includes medical information and data relating to gender, religion, race, sexual orientation, trade union membership and criminal records and proceedings. Where sensitive personal data is processed by the School, the explicit consent of the worker will generally be required in writing.

5.4 Any member of staff collecting or in any way working with personal data must adhere to the following procedures:

(a) When collecting personal data, be clear in your own mind as to why you are collecting this data and what you intend to do with it
(b) If personal data is used for a purpose other than its original intent, it must not be processed for any purpose that is incompatible with the original purpose or purposes
(c) Your department should only hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual, and you should not hold more information than you need for that purpose
(d) You should always take reasonable steps to ensure the accuracy of any personal data you obtain
(e) You should consider any difficulties in keeping the data accurate and current (and assess if keeping the data accurate is indeed necessary)
(f) You will review the length of time that any personal data is kept in relation to the purpose or purposes for which it is held

(g) You will always consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it

(h) You will delete any information that is no longer needed for its original purpose (archiving out of date data where appropriate)

(i) You should inform any data subject if you intend to transfer their information to a third party

(j) Physical copies of files should be kept in a secure area and never left unattended on a desk in a public area

6 Photography

6.1 When dealing with photography staff must adhere to the following guidelines.

(a) When taking photographs for official School use/marketing or for publication to the School website/portal (or any website) the subjects should have been informed of the intended use. It is sufficient to provide this as a written or verbal communication

(b) Photographs or videos of pupils can be used for marketing purposes without explicit parental consent as parents are given warning of this via the Parent Contract, but their names should NOT be linked to the images. The School office can advise if any parents have explicitly asked for photos of their children NOT to be taken or used.

(c) Staff must never take pictures of students using their personal camera or mobile device unless they have been given permission to do so by a member of the senior team and the images are promptly removed/downloaded at the earliest opportunity

(d) Photographs should be deleted when the original purpose is no longer valid

6.2 For further guidance on photography please refer to the School's Photo and Images policy.

7 Social Media

11. Use of Social Media for School Purposes

7.1 The use of social media by the general staff body for Wakefield Independent School purposes is not permitted except by designated members of staff, on the School's Social Media Accounts.

12. Personal use of Social Media

7.2 Staff must be aware that their role comes with particular responsibilities and they must adhere to the School's strict approach to social media.

7.3 Staff must:

(a) Ensure that wherever possible their privacy settings on social media sites are set so that pupils cannot access information relating to their personal lives

(b) Obtain the prior written approval of the Head, to the wording of any personal profile which you intend to create where the School is named or mentioned on a social networking site.

(c) Seek approval from the Head before they speak about or make any comments on behalf of the School on the internet or through any social networking site

(d) Report to their Head of Department or Line Manager immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the School

(e) Immediately remove any internet postings which are deemed by the School to constitute a breach of this or any other School policy. Staff who fail to remove such posts may be subject to disciplinary action

(f) Consider whether a particular posting puts their effectiveness as a teacher at risk

(g) Post only what they want the world to see.

7.4 Staff must not:

(a) Provide references for other individuals, on social or professional networking sites, as such references whether positive or negative can be attributed to the School and create legal liability for both the author of the reference and the School

(b) Post or publish on the internet or on any social networking site, any reference to the School, your colleagues, parents or pupils

(c) Use commentary deemed to be defamatory, obscene, proprietary, or libellous. Staff must exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations

(d) Discuss pupils or colleagues or publicly criticise the School or staff

(e) Post images that include pupils

(f) Initiate friendships with pupils, parents, guardians or carers on any personal social network sites

(g) Accept pupils as friends on any such sites; staff must decline any pupil-initiated friend requests

(h) Associate a work email address with any personal social media accounts

7.5 The School recognises that staff may work long hours and occasionally may desire to use social media for personal activities at the office or by means of our computers, networks and other IT resources and communications systems. We authorise such occasional use so long as it does not involve unprofessional or inappropriate content, and does not interfere with your employment responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the School's business are also prohibited. Staff must ensure that their use of social media does not create any breaches of internet security and therefore must be careful to avoid any applications that might interrupt our IT systems. Excessive use of social media that interrupts staff productivity will be subject to a disciplinary procedure, consistent with this policy.

13. Monitoring of Social Media

7.6 We reserve the right to monitor, intercept and review, without further notice, staff activities using the School's IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes, and you consent to such monitoring by your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

7.7 Do not use the School's computers, telephony, (except for telephones provided in staff rooms) or hosted communication platforms (such as email and intranet) for any matter that you wish to be kept private or confidential from the organisation.

14. Social Media and the End of Employment

7.8 If a member of staff's employment with the School should end, for whatever reason, any personal profiles on social networking sites should be immediately amended to reflect the fact that you are no longer employed or associated with the School.

7.9 All professional contacts that a member of staff has made through their course of employment with the School belong to the School, regardless of whether or not the member of staff has made social media connections with them.

8 Lost Data

8.1 Security breaches must be reported to the Data Protection Officer and dealt with immediately.

(a) Actions that must be carried out include:

(b) Devise a recover and damage limitation plan

(c) Inform appropriate people and organisations

(d) Review response and update information security

9 Data Access Requests

9.1 Data access requests should be passed to the Data Protection Officer.

9.2 Staff should note that there is no requirement to use the words ‘access request’ or ‘data protection’ when making a request. An email asking for ‘all records you have on me’ for example is sufficient to be classed as valid subject access request.

9.3 Staff should note that ANY comment made in a School email or document can potentially be disclosed. There is NO EXEMPTION for ‘embarrassing’ comments made about another individual.

10 Personal Data Overseas

10.1 No personal data should be taken overseas (outside of the EU) unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals when processing their personal data.

10.2 Any member of staff who plans to travel to a country outside of the EU with School data must inform the Data Protection Officer.

11 Breach of Policy

11.1 Any breaches of this policy may result in disciplinary action, and for more serious breaches dismissal.

12 Central Data Retention Periods

15. Bursary

12.1 Correspondence to be destroyed after 10 years
12.2 Digital financial records to be destroyed after 10 years
12.3 Invoices and petty cash slips to be destroyed after 6 years

16. School Office

12.4 Student paper files to be destroyed after 7 years.
12.5 Correspondence and digital files to be destroyed after 10 years

17. General – all other departments or data types

12.6 Paper & digital files containing personal data to be destroyed after 10 years

13 Data Protection Principles

13.1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

13.2 at least one of the conditions in Schedule 2 is met, and
13.3 in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

13.4 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.

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

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

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

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

13.9 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.

13.10 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.