Thomas Jones Primary School

Data Protection and Freedom of Information Policy

The Governing Body of Thomas Jones School adopted this Data Protection and Freedom of Information Policy on 18th June 2018. We will ensure that we are registered with the Information Commissioner's Office and will update notifications annually. The full policy will be reviewed biennially.

Data Protection Officer	Emma Jones
Deputy Data Protection Officer	Yvonne Hoy

Objectives
Our Data Protection and Freedom of Information Policy aims to provide clear practical procedures on information governance for staff and governors in line with the Data Protection Act, 2018, General Data Protection Regulations, 2018 and Freedom of Information Act, 2000.

At Thomas Jones school we comply with all principles of the General Data Protection Regulations, 2018 (GDPR) and promote a positive data protection and security culture that is endorsed by senior leadership and the governing body.

In accordance with legislation this policy applies to all data subjects (individuals) that we hold personal information about and all forms of information regardless of the way it is collected, used, recorded, stored or destroyed and irrespective of whether it is held in paper files or electronically.

Individuals Rights
All personal data relating to staff, pupils or other people with who we have contact, whether held on computer or in paper files, is covered by the GDPR. This includes information about pupils and families, staff and governors, professional experts, suppliers, enquirers and individuals captured by CCTV images. At Thomas Jones we ensure that we adhere to the principle of individual rights and that all individuals have the right to:

- Be informed
- Have access
- Rectify their data
- Erasure of their data (if not required by lawful basis to perform a task in the public interest)
- Restrict processing
- Data portability
- Object to data processing
- Not be subject to automated decision making including profiling

Data Protection Principles
All personal information is handled in line with data protection principles. If processing of personal information is carried out by others on our behalf we ensure that they follow the data protection principles and do so correctly.

At Thomas Jones we are committed to the implementation of the six privacy principles set out in the GDPR. These are:

- Lawfulness, fairness and transparency
- Purpose Limitation
- Data minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality

Privacy Notice

The first principle of data protection is that personal data must be processed fairly and lawfully and processing activity should be transparent. The Data Protection Act, 2018, says that in order for processing to be fair, the data controller (the organisation in control of processing the data) has to make certain information available to the data subjects (the individuals whom the data relates to), so far as practicable, including:

- who the data controller is;
- the purpose or purposes for which the information will be processed; and
- any further information which is necessary in the specific circumstances to enable the processing to be fair.

This applies whether the personal data was obtained directly from the data subjects or from other sources.

At Thomas Jones we have Privacy Notices for staff/governors and also for pupils and their families that clearly state how we meet the GDPR in all processing activity that involves personal data. This is published on our website and circulated to all families, staff and governors annually. (See Appendices 1 and 2)

Information Processing

Purposes for Processing Information

At Thomas Jones we collect and use personal data for the following purposes:

- To support pupil learning
- To monitor and report on pupil attainment and progress
- For employment contract and to manage pay
- To enable a comprehensive picture of the workforce and how it is deployed
- To provide pastoral care
- To assess the quality of our services
- To keep children safe
- To meet our statutory duties placed upon us by the Department for Education
- To comply with the law regarding data sharing

Categories of Personal Data

Categories of personal data that we collect and process include:

- **Identity and Contact Data** (such as name, marital status, date of birth, gender, unique pupil number, contact details and address)
- **Characteristic Data** (such as ethnicity, language, free school meal eligibility)
- **Employment Data** (such as contracts, roles and remuneration details)
- **Safeguarding Data** (such as professional involvement, court orders, criminal record information)
- **Special Educational Needs and Disabilities (SEND) Data** (such as

needs and ranking)
- **Medical and Administration Data** (such as doctors information, health issues, dental health, allergies, medication and dietary requirements)
- **Attendance Data** (such as absences and reasons for absence, previous schools attended)
- **Assessment and Attainment Data** (such as KS1 and 2 SATs test results, phonics check, assessment test results, attainment trackers, appraisal data)
- **Profile Data** (may include your username and password, feedback and survey responses)
- **Behaviour Information** (such as incident reports, behaviour books/plans, exclusions, disciplinary data)
- **Transaction Data** (such as records of uniform purchased and ParentPay transactions)
- **Evaluation Data** (such as parental and pupil feedback on aspects of the school)
- **Photo/Video Data**

This list is not exhaustive; the current list of information we process is available in our school Data Audit. (See Appendix 3)

We also use CCTV systems to monitor and collect visual images for security and the prevention of crime.

Lawful Basis for Processing Personal Data

Article 6 of the GDPR sets out the possible lawful basis and conditions of processing personal data. At least one of the lawful basis for processing personal data must apply whenever we process personal data. These are as follows:

a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
c) Legal Obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
d) Vital Interests: the processing is necessary to protect someone's life.
e) Public Task: the processing is necessary for you to perform a task in the public interest or for your **official functions**, and the task or function has a clear basis in law.
f) Legitimate Interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. This cannot apply if you are a public authority processing data to perform your official tasks. Public authorities will need to rely on official functions.

Special Category Data

Special category data is set out in Article 9 of the GDPR and is defined as data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, health, trade-union membership, genetics, biometrics and sex life or sexual orientation. Data relating to criminal offences is also afforded similar special protection.

At Thomas Jones we treat all information about children's services interactions, free school meal status, pupil premium eligibility, elements of special educational need and disability information, safeguarding information, Children in Need and Children Looked After and some behaviour data with the same 'high status' as the special categories set out in law. This ensures we afford extra protection in terms of the reasons we need to access and process this data.
When processing special category data as well as ensuring we have a lawful basis for processing we also ensure that one of the following conditions for processing applies:

a) **the data subject has given explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.
b) processing is necessary for the purposes of **carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law** in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
c) **processing is necessary to protect the vital interests of the data subject or of another natural person** where the data subject is physically or legally incapable of giving consent.
d) processing is carried out in the course of its **legitimate activities** with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
e) processing relates to personal data which are **manifestly made public** by the data subject.
f) processing is necessary for the establishment in order to exercise or defend **legal claims** or whenever courts are acting in their judicial capacity.
g) **processing is necessary for reasons of substantial public interest,** on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
h) processing is necessary for the **purposes of preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional.
i) processing is necessary for **reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
j) processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) based on Union or Member State law which

shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Safeguarding

GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards will be in place.

Consent

Where a lawful basis requires us to process data, consent is not sought. However where no other legal basis applies we will positively seek individual's consent to process their personal data.

When relying on consent to process data our method of obtaining it will be:

- clearly communicated
- to ask individuals to positively opt-in
- to give sufficient information for individuals to make a choice
- to explain the different ways we will use individual's information
- to provide a clear and simple way for them to indicate they agree to different types of processing

At Thomas Jones school we currently seek consent from parents/carers to take photographs and videos of children to be used for the school website, by other parents/carers during class assemblies or concerts, for class photographs, for requests from outside agencies and to be retained and used once the child has left Thomas Jones school. This consent is obtained via consent forms at the point when children join the school and is then stored in class folders in locked filing cabinets. Consent forms offer parents/carers an opt-in tick box for each option, consent is not assumed. To ensure we meet the General Data Protection Regulations we will have re-obtained consent from all parents/carers using our updated photo/video consent form in June 2018. (See Appendix 4). Consent is gained similarly from staff/governors to use their photographs or video footage on our school website and for requests from outside agencies.

We also obtain consent to send email reminders generated from ParentPay (parent/carer's cashless banking system for school lunches) in order to chase monies owed. This again is sought when parents first log into a ParentPay account and is stored in class folders in locked filing cabinets. Both consent forms can be updated or revoked at any time at the request of the parent/carer or staff member.

We will not publish personal data in newsletters, on our school website or other media without the consent of the data subject.

Data Sharing

From time to time schools are required to pass on personal data to the Local Education Authority (LEA), the Department for Education (DfE) and agencies such as Ofsted and the Standards and Testing Agency as prescribed by law. The

Department of Education may share information about pupils with third parties who promote the education or well-being of children in England. The department has robust processes in place to ensure that the security and confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in electronic format on the National Pupil Database. The law that allows this is the Education (information About Individual Pupils) (England) Regulations 2013.

At Thomas Jones we are the data controller (organisation who determine the purpose and manner in which data are processed). Sometimes we act as joint controller with the LA or DfE as detailed above. Third party data processors are the people or organisations who process data on our behalf or orders. We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. We only provide basic pupil information to our information system contractors such as ParentPay. Others who process or use personal information on the school's behalf must ensure that they follow the principles set out in this policy at all times.
Third party data processors that we use at Thomas Jones include:

- ParentPay
- Caterlink catering suppliers
- Jartech
- PW Payroll Solutions Ltd
- Cool Milk
- School Journey Association
- 3BM
- Health Services
- Educational Psychologist
- Speech and Language Professionals
- SEND Professionals
- KALO Sports Provider
- Play Therapist
- School Photographer

As data controller we ensure that our third party data processors and their sub processors process data on our behalf in line with the GDPR. We hold copies of their privacy notices to evidence compliance with the GDPR or have Data Sharing Agreements in place to confirm that processors will adhere to our policy and privacy notice (See Appendix 5).

CCTV

At Thomas Jones we have a CCTV system to monitor the main entrance to the school, the vehicle entrance and other key locations within the grounds. Images of people are covered by data protection along with information derived from images. CCTV footage is stored in a secure location within the school and all footage is automatically deleted after three weeks. The equipment is installed and managed by Chubb but Chubb do not view or retain any CCTV footage taken on the premises. If CCTV footage is needed to be reviewed at the school, this will be done so in a secure location by two members of staff at all times. The only third party that would have

immediate access to CCTV footage would be the police to support them with any enquiries. Any other third parties monitoring our CCTV images would need a legitimate reason and a contract in place ensuring they meet all the requirements of the GDPR before they could view any footage. No third parties are able to distribute or remove personal data in the form of CCCTV images unless under legal duties (police).

Cookies Policy
The Thomas Jones school website www.thomasjones.co.uk uses cookies to track repeat visitors and new visitors to the website only but does not collect any personal data. A cookie disclaimer and consent flashes up as soon as a visitor visits our website.

Data Audit
At Thomas Jones we have compiled a detailed data audit to demonstrate how we have integrated data protection into our processing activity. (See Appendix 3). The audit contains details of all personal data we process, what the data is processed for, the lawful basis for processing data, retention periods and secure storage. This will be evaluated by the Data Protection Officer every 6 months to review retention periods and ensure all details are current and correct.

Security of Personal Information
We regularly review the physical security of the school building and storage systems, and access to them. This includes the storage of paper records and the equipment used to store and process information electronically.

At Thomas Jones we ensure that personal information is kept secure in the following ways:

- Paper documents are kept in secure locked cupboards.
- Privacy notices or Data Sharing Agreements for our third party processors are held to ensure they comply with the GDPR.
- Personal information is not allowed to leave the school premises unless encrypted.
- Strong passwords are ensured for any electronic equipment holding personal information.
- A DPO oversees data security in the school.
- All governors and staff have read our Data Protection and Freedom of Information Policy and adhere to this.
- Our network is protected by an up to date firewall and comprehensive anti-virus and anti-malware software.
- External penetration tests on our network are performed to ensure we remain protected against malicious attack.
- We have active network monitoring processes in place to detect any unusual activity.
- Data Protection Impact Assessments are completed before any new project is undertaken involving personal data.
- Staff will log on remotely and securely if working outside of the school premises. If staff are unable to log on remotely work involving any personal data will only be taken from the school site on an encrypted USB storage device.

- Staff will ensure that no personal data is left open on computers that could be accessed by another individual.
- No USB storage devices are able to be used except a school encrypted memory stick. All other USB devices will be banned from the school network.
- If school laptops are taken out of school no data will be stored on these. Laptops but will only be utilized to access the network remotely.
- Idle workstations will automatically be locked after 5 minutes for administration staff and 15 for teaching staff.
- Supply staff and visitors will be provided with a temporary login to access the shared drive only. The login will expire after 24 hours.

Subject Access Requests (SAR)

All people for whom we hold personal information have a right under the 2018 Data Protection Act and the GDPR to access personal data being kept about them in either electronic or paper form; the right of subject access. This is subject to certain exemptions. Any individual is able to submit a Subject Access Request (SAR) at any time in order to request their personal data that we hold at Thomas Jones. Parent/carers can make a subject access request on behalf of their child. We ask that all SAR's are put in writing either by letter or email to the school detailing the specific data information that is being requested. We are aware that a SAR might be referred to differently and will identify this and respond appropriately completing a Subject Access Request Report. (See Appendix 6).

Once a SAR has been received the school will ensure that they comply with the request within 30 days following receipt of the request and the provision of photo identification. A Subject Access Request Record will immediately be completed by the school to record all details of the request If a SAR is sent to the school during the school holidays the school will address this as soon as the school re-opens. An automated response to all emails sent to the school email address will specify this.

In line with the GDPR, we hold the right to refuse or charge for requests that are manifestly unfounded or excessive. If a large volume of data is held we may need to ask the data subject to specify precisely what the request relates to.

If a request is refused, we will within 30 days write to the individual explaining why we have refused the request and explain that they have the right to complain to the ICO.

Only in exceptional cases would we withhold some of the information which is requested by an individual. For example, if disclosure of that information might cause harm to the physical or mental health of the individual, or if information may identify third parties and in the case of data disclosure hindering the prevention and detection of crime or the prosecution or apprehension of offenders.

Educational Records

Any request for a pupil's educational record will be acted upon in line with the Education Regulations. Response to these requests will be within 15 school days.

Freedom of Information

The Freedom of Information Act, 2000, affords individuals and organisations the right of access to know of and receive all recorded information such as minutes of meetings, policies, procedures, records and reports (not personal data- this would be

obtained through a Subject Access Request). We will ensure that we meet these requirements in the case of any Freedom of Information request within 20 calendar days of receipt of the request. As with a SAR we ask that Freedom of Information requests are made in writing to the school or via email. At Thomas Jones we have an approved publication scheme in line with the Freedom of Information Act, 2000, and Local Authority Model Publication scheme. (See Appendix 7) We ensure that we reply to requests for information in line with this legislation.
In line with the Freedom of Information Act, we notify staff of any personal information that would be provided about them when answering a Freedom of Information request.

Rectification, Retention, Erasure and Disposal
At Thomas Jones we ensure that data is kept up to date. Our Data Audit holds details of retention periods for all data held and is reviewed by the Data Protection Officer every 6 months. Data retention periods are set in line with the guidance by the London Grid for Learning. When a data retention period expires data is erased and destroyed by secure methods. This includes deletion from electronic records and the shredding of any paper records using a cross-cut shredder.
In our Privacy Notice, that is shared annually, we request families, staff and governors to inform us of any changes that need rectifying to their personal data.
Data subjects are able to make requests to the school administrator (Deputy DPO) for information to be rectified or deleted at any point. If a data subject approaches us for these matters a Data Rectification and Withdrawal Report (see Appendix 8) is completed with full details of the action. This will be completed in collaboration with the Data Protection Officer.
The Data Protection Officer or Deputy at the school will make all decisions about deleting data held at the school. This is then kept on file as a record of the data processing activity. The same form is utilised for data subjects to withdraw consent for any data where the legal basis is consent. The form is then attached to all original documents and updated on the original form.

Monitoring Data Protection Compliance
The DPO will audit our compliance of the GDPR every 6 months, checking the school Data Audit and procedures to ensure the security of all personal data held at Thomas Jones. The Local Authority should also have a Data Protection Officer. The school will request the Local Authority DPO to visit and audit our compliance with the GDPR.

Data Protection Impact Assessment (DPIA)
Where a new project involving the processing of personal data is to take place or if a data processing activity is 'likely to result in a high risk to the rights and freedoms of natural persons' we will carry out a Data Protection Impact Assessment (DPIA) to try to diminish or withdraw risks in accordance with the accountability principle in the GDPR. If we are unsure whether a DPIA is required we will complete one to ensure that we are compliant (See Appendix 9 Data Protection Impact Assessment Record). If we assess whether a DPIA is required but decide not to continue with the process we will keep records of our reasons and will keep the processing activity under review to assess whether there are any changes to the risk which means that a DPIA is required at a later date. If the data processing activity is being undertaken by a third

party data processor the processor will be expected to support the school in completing the DPIA.

High Risk Processing
Processing activities that are classified as 'high risk' require a DPIA in place.

High risk processing includes:
- Evaluation or scoring
- Automated decision-making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative use of or applying a new-technological or organizational solution
- Preventing data subjects from exercising a right or from using a service or contract

In most cases a combination of two of these high risk processing activities would instigate a DPIA taking place but in some cases one factor is sufficient.

The GDPR states that in the completion of a DPIA not all risks need to be eliminated but an assessment of how risks can be minimised or whether any remaining risks are justified needs to take place. If following a DPIA the data processing activity is deemed to remain high risk and we have been unable to minimise or eliminate these risks we will consult the Information Commissioners Officer (ICO) before any processing commences.
It is recommended that DPIAs are carried out for the use of CCTV within schools. We have adhered to this recommendation and have reduced risks from high to medium. Any further recommendations for DPIAs will be completed by the DPO.

Business Risk Register
At Thomas Jones we will assess and identify areas that could cause data protection or security compliance problems and will record these on our business risk register. We will apply controls and test these controls to ensure security of personal data and compliance with the GDPR.

Data Breaches
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration unauthorised disclosure of, or access to personal data. This includes breaches that are the result of both accidental and deliberate causes. At Thomas Jones we have procedures to detect, report and investigate any personal data breach.
Our Data Protection Officer and Deputy Data Protection Officer monitor the security of all data on a regular basis in consultation with the Computing Leader. If a breach is reported, suspected or identified a Data Breach Report (See Appendix 10) will be completed to itemise all actions that need to be taken to address the breach. All staff know to report any data breaches immediately to the DPO or Deputy Officer.
We are legally obliged to report any breaches to the ICO within 72 hours, where feasible, if a data breach if unaddressed is likely to have a significant detrimental

effect on individuals or if there's a high risk to the rights and freedoms of any individual. Data breaches will be reported to data subjects in the same manner.

If a breach occurs during the school holidays or at a weekend staff must report the breach to the DPO straight away if possible, they will then contact the ICO if required and complete the Data Breach Record. If the DPO or Deputy DPO are unavailable the Headtacher or Deputy should be notified.

Staff and Governor Responsibilities

Staff and Governors at Thomas Jones are trained in the principles of data protection and have read and adhere to our Data Protection and Freedom of Information policy. Staff responsibilities include:

- A duty of confidentiality.
- Signing and adhering to the school's Acceptable Use Agreement (AUA) when employment commences and again each time the AUA is updated.
- The use of complex passwords for email and computer systems that are kept secure, regularly changed and never shared.
- Never taking personal data from the school premises unless saved on an encrypted memory stick.
- The use of complex passwords to secure devices if accessing personal data remotely and ensuring no other person at any time has access to this data.
- Ensuring sensitive or personally identifiable data is not sent via email across different email systems and is only shared via secure methods to professional's validated accounts.
- Ensuring no personal online services are set up or utilised for school data and only work email accounts are used.
- The clearing of deleted files once data is deleted.
- The use of screen locks to protect data on computers at all times when not in use.
- Ensuring all cupboards that store personal data are kept locked and secure at all times with keys that are only held by named staff.
- Assessing whether a DPIA is required at the early stages of a project involving personal data.
- Setting profiles on all personal social networking sites to protect privacy.
- Marking meeting notes that include sensitive personal data with a 'securely destroy' header or footer and ensuring documents are securely destroyed using a cross-cut shredder immediately after use.
- Including data protection statements on any forms that are used to collect personal data.
- Responsibility for the security of their log in details.
- Immediately reporting any suspicion, or evidence, that there has been a breach of security.
- Never using personal devices (cameras, mobile phones) to take photos or videos of pupils, families or staff.
- Ensuring they follow whether consent is obtained or denied in organising photographs and video footage taken and used within the school.

Governor responsibilities include:

- A duty of confidentiality.
- Signing and adhering to the school's Acceptable Use Agreement (AUA) when employment commences and again each time the AUA is updated.
- The use of complex passwords for email and computer systems that are kept secure, regularly changed and never shared.
- Ensuring sensitive or personally identifiable data is not sent via email across different email systems and is only shared via secure methods to professional's validated accounts.
- Ensuring no personal online services are set up or utilised for school data and only work email accounts are used.
- Setting profiles on all personal social networking sites to protect privacy.
- Immediately reporting any suspicion, or evidence, that there has been a breach of security.
- Never using personal devices (cameras, mobile phones) to take photos or videos of pupils, families or staff.

Supply staff will not have access to the full school IT system, will sign a AUA when they arrive at the school and will be provided with a temporary login that will expire after 24 hours. Personal data will only be made available on a need to know basis.

Any failure to follow the policy or if staff are careless or reckless with data can result in disciplinary proceedings.

Working Remotely

For staff members working remotely the school Acceptable Use Agreement covers the GDPR principles. For staff taking IT equipment to use outside of the school grounds a loan agreement form needs to be signed to confirm that they will use this in line with the GDPR.

Use of Mobile Devices for Work Purposes

For staff members that access emails using an app or other personal data on a mobile device they must ensure that the app being used is password protected, that their mobile device also has a secure lock and that it is registered with Jartech as a work device. In the event of their mobile device being lost or stolen Jartech must be informed straight away so that the device can be wiped of all data. Staff must be made aware that this is the procedure in case of a lost or stolen device and ensure that if this is a personal device that all other personal data is saved regularly to avoid loss.

Data Protection Training and Awareness

All staff and governors of Thomas Jones have been trained in data protection to ensure we are compliant with the Data Protection Act, the GDPR and Freedom of Information Act and that all staff are aware of changes related to data protection. Policy is approved by the full governing body and is shared with all staff, inclusive of catering, cleaning and administrative staff. Staff are kept abreast of any updates at regular staff meetings.

Staff and Governors are aware of their role relating to data protection and who to report any concerns to regarding data protection security within the school.

Staff training encourages personal responsibility and good security behaviours as well as educating staff on their data protection and security responsibilities and promoting data protection and security awareness and compliance.

Emma Jones
May 2018