The Boleyn Trust

Data Protection Policy

Table of Contents

01. POLICY STATUS AND REVIEW

Policy Owner:	Chief Finance and Operating Officer
Policy Author:	Chief Finance and Operating Officer
Approver:	Board of Trustees
Last Review:	August 2023
New Review:	August 2024
Ratified:	September 2023

The Board of Trustees has agreed to this Policy and, as such, it applies to all Schools within the Trust. Please note that should any further national guidance be issued by external agencies that are relevant to this policy, it will be updated accordingly prior to the review date shown below and re-circulated.

Please Note:

Boleyn Trust CEO and Accounting Officer:	**Tom Canning CBE**
Boleyn Trust Chief Finance and Operating Officer:	**Steven Lock**
Boleyn Trust Head of ICT and Data Security:	**Ladi Kelekun**
Boleyn Trust Data Protection Officer:	**Judicium Consulting Limited**

……

Chair of the Board of Trustees

02. DATA PROTECTION POLICY

2.1 INTRODUCTION

The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed, or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure, or destruction of personal data.

The Boleyn Trust (the "Trust") will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

2.2 DEFINITIONS

2.2.1 Personal data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

2.2.2 Special Category Data

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

2.2.3 Data Subject

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

2.2.4 Data Controller

The organisation storing and controlling such information (i.e., the Trust) is referred to as the Data Controller.

2.2.5 Processing

Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

2.2.6 Automated Processing

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

2.2.7 Data Protection Impact Assessment (DPIA)

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

2.2.8 Criminal Records Information

This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

2.3 WHEN CAN THE TRUST PROCESS PERSONAL DATA

2.3.1 Data Protection Principles

The Trust are responsible for and adhere to the principles relating to the processing of personal data as set out in the UK GDPR.

The principles the Trust must adhere to are set out below.

2.3.1.1 Principle 1: Personal Data

Personal data must be processed lawfully, fairly and in a transparent manner.

The Trust only collect, process and share personal data fairly and lawfully and for specified purposes.

The Trust must have a specified purpose for processing personal data and special category of data as set out in the UK GDPR.

Before the processing starts for the first time we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

The Trust may only process a data subject's personal data if one of the following fair processing conditions are met:

- The data subject has given their consent.
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract.
- To protect the data subject's vital interests.
- To meet our legal compliance obligations (other than a contractual obligation).
- To perform a task in the public interest or in order to carry out official functions as authorised by law.
- For the purposes of the Trust's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

2.3.1.2 Special Category Data

The Trust may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met:

- The data subject has given their explicit consent.
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the Trust in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay.
- To protect the data subject's vital interests.
- To meet our legal compliance obligations (other than a contractual

obligation).

- Where the data has been made public by the data subject.
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law.
- Where it 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.
- Where it is necessary for reasons of public interest in the area of public health.
- The processing in necessary for archiving, statistical or research purposes.

The Trust identifies and documents the legal grounds being relied upon for each processing activity.

2.3.2.3 Consent

Where the Trust relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the Trust will normally seek another legal basis to process that data. However if explicit consent is require the data subject will be provided with full information in order to provide explicit consent.

The Trust will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

2.3.3 Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes.

Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

The Trust will not use personal data for new, different or incompatible purposes

from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

2.3.4 Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The Trust will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the Trust shall delete or anonymise the data. Please refer to the Trus's Data Retention Policy for further guidance.

2.3.5 Principle 4: Personal data must be accurate and, where necessary, kept up to date

The Trust will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the Trust.

2.3.6 Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Trust will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the Trust's Retention Policy for further details about how the Trust retains and removes data.

2.3.7 Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

In order to assure the protection of all data being processed, the Trust will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as:

- Encryption.
- Pseudonymisation (this is where the Trust replaces information that directly or indirectly identifies an individual with one or more artificial

identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure).

- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it).
- Adhering to confidentiality principles.
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The Trust follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The Trust will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Full details on the Trust's security measures are set out in the Trust's Security Policy.

2.4 SHARING PERSONAL DATA

The Trust will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party:

- Has a need to know the information for the purposes of providing the contracted services.
- Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained.
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place.
- The transfer complies with any applicable cross border transfer restrictions.
- A fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the Trust is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our Trust shall be clearly defined within written notifications and details and basis for sharing that data given.

2.5 TRANSFER OF DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

The Trust will not transfer data to another country outside of the EEA without appropriate

safeguards being in place and in compliance with the UK GDPR. All staff must comply with the Trust's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

2.6 TRANSFER OF DATA OUTSIDE OF THE UK

The Trust may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, standard data protection clauses or compliance with an approved code of conduct.

2.7 DATA SUBJECT'S RIGHTS AND REQUESTS

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the Trust handle their personal data are set out below:

(a) (Where consent is relied upon as a condition of processing) to withdraw consent to processing at any time.
(b) Receive certain information about the Trust's processing activities.
(c) Request access to their personal data that we hold (see "Subject Access Requests").
(d) Prevent our use of their personal data for marketing purposes.
(e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data.
(f) Restrict processing in specific circumstances.
(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest.
(h) Request a copy of an agreement under which personal data is transferred outside of the EEA.
(i) Object to decisions based solely on automated processing.
(j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else.
(k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.
(l) Make a complaint to the supervisory authority.
(m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the Trust to verify the identity of the individual making the request.

2.8 DIRECT MARKETING

The Trust are subject to certain rules and privacy laws when marketing. For example a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The Trust will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The Trust will promptly respond to any individual objection to direct marketing.

2.9 EMPLOYEE OBLIGATIONS

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the Trust in the course of their employment or engagement. If so, the Trust expects those employees to help meet the Trust's data protection obligations to those individuals. Specifically, you must:

- Only access the personal data that you have authority to access, and only for authorised purposes.
- Only allow others to access personal data if they have appropriate authorisation.
- Keep personal data secure (for example by complying with rules on access to Trust premises, computer access, password protection and secure file storage and destruction [Please refer to the Trust's Security Policy for further details about our security processes]).
- Not to remove personal data or devices containing personal data from the Trust premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;
- Not to store personal information on local drives.

2.10 ACCOUNTABILITY

The Trust will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

The Trust have taken the following steps to ensure and document UK GDPR compliance:

Appointed a Data Protection Officer (DPO)

Data Protection Officer:	Judicium Consulting Limited
Address:	72 Cannon Street, London, EC4N 6AE
Email:	dataservices@judicium.com
Web:	www.judiciumeducation.co.uk
Telephone:	0203 326 9174
Lead Contact:	Craig Stilwell

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) If you are unsure of the lawful basis being relied on by the Trust to process personal data.
(b) If you need to rely on consent as a fair reason for processing (please see below the

section on consent for further detail).

(c) If you need to draft privacy notices or fair processing notices.

(d) If you are unsure about the retention periods for the personal data being processed [but would refer you to the Trust's retention policy in the first instance].

(e) If you are unsure about what security measures need to be put in place to protect personal data.

(f) If there has been a personal data breach [and would refer you to the procedure set out in the Trust's breach notification policy].

(g) If you are unsure on what basis to transfer personal data outside the EEA.

(h) If you need any assistance dealing with any rights invoked by a data subject.

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for.

(j) If you plan to undertake any activities involving automated processing or automated decision making.

(k) If you need help complying with applicable law when carrying out direct marketing activities.

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

2.11 PERSONAL DATA BREACHES

The UK GDPR requires the Trust to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches. This is your schools Data Protection Champion or in their absence the Chief Finance and Operating Officer of the Trust.

2.12 TRANSPARENCY AND PRIVACY NOTICES

The Trust will provide detailed, specific information to data subjects. This information will be provided through the Trust's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices sets out information for data subjects about how the Trust use their data and the Trust's privacy notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR including the identity of the data protection officer, the Trust's contact details, how and why we will use, process, disclose, protect and retain personal data. This will be provided in our privacy notice.

When personal data is collected indirectly (for example from a third party or publically available source), we will provide the data subject with the above information as soon as possible after receiving the data. The Trust will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as “children” under the UK GDPR.

2.13 PRIVACY BY DESIGN

The Trust adopt a privacy be design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Trust takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

2.14 DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

In order to achieve a privacy by design approach, the Trust conduct DPIAs for any new technologies or programmes being used by the Trust which could affect the processing of personal data. In any event the Trust carries out DPIAs when required by the UK GDPR in the following circumstances:

- For the use of new technologies (programs, systems or processes) or changing technologies.
- For the use of automated processing.
- For large scale processing of special category data.
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain:

- A description of the processing, its purposes and any legitimate interests used.
- An assessment of the necessity and proportionality of the processing in relation to its purpose.
- An assessment of the risk to individuals.
- The risk mitigation measures in place and demonstration of compliance.

2.15 RECORD KEEPING

The Trust are required to keep full and accurate records of our data processing activities.

These records include:

- The name and contact details of the Trust.
- The name and contact details of the Data Protection Officer.
- Descriptions of the types of personal data used.
- Description of the data subjects.
- Details of the Trust’s processing activities and purposes.
- Details of any third party recipients of the personal data.
- Where personal data is stored.
- Retention periods.
- Security measures in place.

2.16 TRAINING

The Trust will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

2.17 AUDIT

The Trust through its data protection officer regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

2.18 MONITORING

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Trust.

2.19 AUTOMATED PROCESSING AND AUTOMATED DECISION MAKING

Generally automated decision making is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) The data subject has given explicit consent.
(b) The processing is authorised by law.
(c) The processing is necessary for the performance of or entering into a contract.

If certain types of sensitive data are being processed, then (b) or (c) above will not be allowed unless it is necessary for the substantial public interest (for example fraud prevention).

If a decision is to be based solely on automated processing, then data subjects must be informed of their right to object. This right will be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the data subject's rights and freedoms and legitimate interests.

The Trust will also inform the data subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the data subject the right to request human intervention, express their point of view or challenge the decision.

The Trust will carry out a data protection impact assessment before any automated processing or automated decision making activities are undertaken.

03. DATA BREACH POLICY

3.1 INTRODUCTION

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The UK GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the Trust of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

3.2 DEFINITIONS

3.2.1 PERSONAL DATA

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

3.2.2 SPECIAL CATEGORY DATA

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences

and convictions.

3.2.3 PERSONAL DATA BREACH

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

3.2.4 DATA SUBJECT

Person to whom the personal data relates.

3.2.5 ICO

ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

3.3 RESPONSIBILITY

The Chief Finance and Operating Officer has overall responsibility for breach notification within the Trust. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

In the absence of the Chief Finance and Operating Officer, please do contact the Chief Executive.

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed.

The DPO's contact details are set out below: -

Data Protection Officer:	Judicium Consulting Limited
Address:	72 Cannon Street, London, EC4N 6AE
Email:	dataservices@judicium.com
Web:	www.judiciumeducation.co.uk
Telephone:	0203 326 9174
Lead Contact:	Craig Stilwell

3.4 SECURITY AND DATA RELATED POLICIES

Staff should refer to the following policies that are related to this data protection policy: Security Policy which sets out the Trust's guidelines and processes on keeping personal data secure against loss and misuse.

Data Protection Policy which sets out the Trust's obligations under UK GDPR about how they process personal data.

These policies are also designed to protect personal data and can be found at

www.theboleyntrust.org.

3.5 DATA BREACH PROCEDURE

3.5.1 WHAT IS A PERSONAL DATA BREACH?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive):

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss).
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (for example sending an email or SMS to the wrong recipient).
- Unforeseen circumstances such as a fire or flood.
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

3.5.2 WHEN DOES IT NEED TO BE REPORTED?

The Trust must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- Potential or actual discrimination.
- Potential or actual financial loss.
- Potential or actual loss of confidentiality.
- Risk to physical safety or reputation.
- Exposure to identity theft (for example through the release of non-public identifiers such as passport details).
- The exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

3.5.3 REPORTING A DATA BREACH

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should:

Complete a data breach report form (which can be obtained from Judicium) and email the completed form to steven.lock@theboleyntrust.org.

Where appropriate, you should liaise with your line manager about completion of

the data report form. Breach reporting is encouraged throughout the Trust and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from the DPO.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The Chief Finance and Operating Officer will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

3.5.4 MANAGING AND RECORDING THE BREACH

On being notified of a suspected personal data breach, the Chief Finance and Operating Officer will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:

- Where possible, contain the data breach.
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed.
- Assess and record the breach in the Trust's data breach register.
- Notify the ICO where required.
- Notify data subjects affected by the breach if required.
- Notify other appropriate parties to the breach.
- Take steps to prevent future breaches.

3.5.5 NOTIFYING THE ICO

The Chief Finance and Operating Officer will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of Trust holidays (I.e. it is not 72 working hours). If the Trust are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

3.5.6 NOTIFYING DATA SUBJECTS

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Chief Finance and Operating Officer will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the Trust have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the

breach, the Chief Finance and Operating Officer will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the Trust will consider alternative means to make those affected aware (for example by making a statement on the Trust website).

3.5.7 NOTIFYING OTHER AUTHORITIES

The Trust will need to consider whether other parties need to be notified of the breach. For example:

- Insurers.
- Parents.
- Third parties (for example when they are also affected by the breach).
- Local authority.
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

3.5.8 ASSESSING THE BREACH

Once initial reporting procedures have been carried out, the Trust will carry out all necessary investigations into the breach.

The Trust will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the Trust will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include:

- What type of data is involved and how sensitive it is.
- The volume of data affected.
- Who is affected by the breach (i.e. the categories and number of people involved).
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise.
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation).
- What has happened to the data?
- What could the data tell a third party about the data subject?
- What are the likely consequences of the personal data breach on the Trust.
- Any other wider consequences which may be applicable.

3.6 PREVENTING FUTURE BREACHES

Once the data breach has been dealt with, the Trust will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- Establish what security measures were in place when the breach occurred.
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again.
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice.
- Consider whether it is necessary to conduct a privacy or data protection impact assessment.
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register.
- To debrief governors/management following the investigation.

3.7 REPORTING DATA PROTECTION CONCERNS

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to the DPO. This can help capture risks as they emerge, protect the Trust from data breaches and keep our processes up to date and effective.

3.8 MONITORING

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Trust.

04. INFORMATION SECURITY POLICY

4.1 INTRODUCTION

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The Trust is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This documents sets out the measures taken by the Trust to achieve this, including to:

- Protect against potential breaches of confidentiality.
- Ensure that all information assets and IT facilities are protected against damage, loss or misuse.
- Support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data.
- Increase awareness and understanding at the Trust of the requirements of information security and the responsibility to staff to protect the confidentiality and integrity of the information that they themselves handle.

Information Security can be defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

Staff are referred to the Trust's Data Protection Policy, Data Breach Policy and Electronic Information and Communication Systems Policy for further information. These policies are also designed to protect personal data.

For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

4.2 SCOPE

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Trust, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with

the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

General principles

All data stored on our IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the Trust's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with their Data Protection Champion the appropriate security arrangements for the type of information they access in the course of their work.

All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by such third party/parties as the Chief Finance and Operating Officer may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the Trust's Head of ICT and Data Security unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the Chief Finance and Operating Officer who shall have the Head of ICT and Data Security investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer and Chief Finance and Operating Officer.

4.3 PHYSICAL SECURITY AND PROCEDURES

Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available [storage rooms, locked cabinets, and other storage systems with locks] shall be used to store paper records when not in use.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of Trust premises.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the Data Protection Champion as soon as possible who will liaise with the Chief Finance and Operating Officer. Increased

risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The Trust and school carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

The School has an intercom system to minimise the risk of unauthorised people from entering the Trust premises.

The School close the School gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.

CCTV Cameras are in use at the School and monitored by Senior Leaders.

Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

4.4 COMPUTERS AND IT

4.4.1 Responsibilities of the Head of ICT and Data Security and School Specific ICT Managers/post holders

The post holder(s], shall be responsible for the following:

a) Ensuring that all IT Systems are assessed and deemed suitable for compliance with the Trust's security requirements.
b) Ensuring that IT Security standards within the Trust are effectively implemented and regularly reviewed, working in consultation with the Trust's management, and reporting the outcome of such reviews to the Trust's management.
c) ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the UK GDPR and the Computer Misuse Act 1990.

Furthermore, the post holder(s) shall be responsible for the following:

a) Assisting all members of staff in understanding and complying with this policy.
b) Providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems.
c) Ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements.
d) Receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the Data Protection Officer].
e) Taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff.
f) Monitoring all IT security within the Trust and taking all necessary action

to implement this policy and any changes made to this policy in the future.

g) Ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

4.4.2 Responsibilities – Members of staff

All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

You must immediately inform your Data Protection Champion of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Breach Notification Policy.

Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the Head of ICT and Data Security who will inform the Chief Finance and Operating Officer immediately.

You are not entitled to install any software of your own without the approval of the Chief Finance and Operating Officer. Any software belonging to you must be approved by the Chief Finance and Operating Officer and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

Prior to installation of any software onto the IT Systems, you must obtain written permission by the Chief Finance and Operating Officer. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

Prior to any usage of physical media (e.g. USB memory sticks or disks of any kind) for transferring files, you must make sure to have the physical media is virus-scanned. The Chief Finance and Operating Officer's approval must be obtain prior to transferring of files using cloud storage systems.

If you detect any virus this must be reported immediately to the Head of ICT and Data Security who will inform the Chief Finance and Operating Officer (this rule shall apply even where the anti-virus software automatically fixes the problem).

4.5 Access security

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

The Trust has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the Trust's network. The Trust also teach

individuals about e-safety to ensure everyone is aware of how to protect the Trust's network and themselves.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the Chief Finance and Operating Officer. Biometric log-in methods can only be used if approved by the Chief Finance and Operating Officer.

All passwords must, where the software, computer, or device allows:

a) Be at least 6 characters long including both numbers and letters.
b) Be changed on a regular basis [and at least every 180 days].
c) Cannot be the same as the previous 10 passwords you have used.
d) Not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.).

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Group who will liaise with the Chief Finance and Operating Officer as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the Trust's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If you forget your password you should notify your schools ICT Technician to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. If necessary you may write down passwords provided that you store them securely (e.g. in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

Computers and other electronical devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this this time period or disable the lock.

All mobile devices provided by the Trust, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the Trust's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

4.6 DATA SECURITY

Personal data sent over the Trust network will be encrypted or otherwise secured.

All members of staff are prohibited from downloading, installing or running software from

external sources without obtaining prior authorisation from the Chief Finance and Operating Officer who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the Trust's systems.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the Trust's Wi-Fi provided that you follow the requirements and instructions governing this use. All usage of your own device(s) whilst connected to the Trust's network or any other part of the IT Systems is subject to all relevant Trust Policies (including, but not limited to, this policy). The Chief Finance and Operating Officer may at any time request the immediate disconnection of any such devices without notice.

4.7 ELECTRONIC STORAGE OF DATA

All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by the Head of ICT and Data Security.

All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

You should not store any personal data on any mobile device, whether such device belongs to the Trust or otherwise without prior written approval of the Chief Finance and Operating Officer. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the Trust's computer network in order for it to be backed up.

All electronic data must be securely backed up by the end of the each working day.

4.8 HOME WORKING

You should not take confidential or other information home without prior permission of the Chief Finance and Operating Officer or Chief Executive, and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you must ensure that:

a) The information is kept in a secure and locked environment where it cannot be accessed by family members or visitors.
b) All confidential material that requires disposal is shredded or, in the case of electronical material, securely destroyed, as soon as any need for its retention has passed.

4.9 COMMUNICATIONS, TRANSFER, INTERNET AND EMAIL USE

When using the Trust's IT Systems you are subject to and must comply with the Trust's Electronic Information and Communication Systems Policy.

The Trust work to ensure the systems do protect pupils and staff and are reviewed and

improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to the schools Data Protection Lead.

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the Trust cannot accept liability for the material accessed or its consequence.

All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email, or sent by tracked DX (document exchange) or recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

Postal, DX, fax and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the Trust.

Personal or confidential information should not be removed from the Trust without prior permission from the Chief Finance and Operating Officer and or the Chief Executive, except where the removal is temporary and necessary. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

a) Not transported in see-through or other un-secured bags or cases.
b) Not read in public places (e.g. waiting rooms, cafes, trains, etc.).
c) Not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.).

4.10 REPORTING SECURITY BREACHES

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Data Protection Champion who will inform the Chief Finance and Operating Officer. All members of staff have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the Chief Finance and Operating Officer and DPO shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Chief Finance and Operating Officer. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, the Chief Finance and Operating Officer.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the Data Protection Champion who will then inform the Chief Finance and Operating Officer.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Breach Notification Policy.

05. CYBER SECURITY POLICY

5.1 INTRODUCTION

Cyber security has been identified as a risk for the Trust and every employee needs to contribute to ensure data security.

The Trust has invested in technical cyber security measures, but we also need our employees to be vigilant and act to protect the Trust IT systems.

The Trust's Head of ICT and Data Security is responsible for cyber security within the Trust.

If you are an employee, you may be liable to disciplinary action if you breach this policy.

This policy supplements other data management and security policies, namely our [Data Protection Policy, Data Breach Policy, Information Security Policy, Acceptable Use Policy, Home Working Policy, Electronic Information and Communications Policy and Clear Desk Policy].

5.2 PURPOSE AND SCOPE

The purpose of this document is to establish systems and controls to protect the Trust from cyber criminals and associated cyber security risks, as well as set out an action plan should the Trust fall victim to cyber-crime.

This policy is relevant to all staff.

5.3 WHAT IS CYBER-CRIME?

Cyber-crime is simply a crime that has some kind of computer or cyber aspect to it. It takes shape in a variety of different forms, e.g. hacking, phishing, malware, viruses or ransom attacks.

The following are all potential consequences of cyber-crime which could affect individuals and/or individuals:

- Cost.
- Confidentiality and data protection.
- Potential for regulatory breach.
- Reputational damage.
- Business interruption.
- Structural and financial instability.

It is important, given the serious consequences above, to be careful not to be the victim of cyber-crime and to follow the guidance within this policy.

5.4 CYBER-CRIME PREVENTION

This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime. The Head of ICT and Data Security can provide further details of other aspects of the Trust/Trust risk assessment process upon request.

The Trust have put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance to staff.

5.5 TECHNOLOGY SOLUTIONS

The Trust have a variety of technical measures in place for protection against cyber-crime. They include:

- Firewalls.
- Anti-virus software.
- Anti-spam software.
- auto or real-time updates on our systems and applications;
- URL filtering.
- Secure data backup.
- Encryption.
- Deleting or disabling unused/unnecessary user accounts.
- Deleting or disabling unused/unnecessary software.
- Using strong passwords.
- Disabling auto-run features.

5.6 CONTROLS AND GUIDANCE FOR STAFF

All staff must follow the policies related to cyber-crime and cyber security as listed in the introduction to this policy.

All staff will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the Trust or any third parties with whom we share data.

All staff must:

- Choose strong passwords.
- Keep passwords secret.
- Never reuse a password.
- never allow any other person to access the Trust's systems using your login details;
- Not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on their computer, phone or network or the Trust IT systems.
- Report any security breach, suspicious activity, or mistake made that may cause a cyber-security breach, to the Head of ICT and Data Security who will then inform the Chief Finance and Operating Officer as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our data breach policy.
- Only access work systems using computers or phones that the Trust owns. Staff may only connect personal devices to the [public] and/or [visitor] Wi-Fi provided.
- Not install software onto your Trust computer or phone. All software requests should be made to the Head of ICT and Data Security and signed off by the Chief Finance and Operating Officer.
- Avoid clicking on links to unknown websites, downloading large files, or accessing

inappropriate content using Trust equipment or networks.

All staff must not misuse IT systems. The Trust considers the following actions to be a misuse of its IT systems or resources:

- Any malicious or illegal action carried out against the Trust or using the Trust's systems.
- Accessing inappropriate, adult or illegal content within Trust premises or using Trust equipment.
- Excessive personal use of Trust's IT systems during working hours.
- Removing data or equipment from Trust premises or systems without permission, or in circumstances prohibited by this policy.
- Using Trust equipment in a way prohibited by this policy.
- Circumventing technical cyber security measures implemented by the Trust's IT team.
- Failing to report a mistake or cyber security breach.

5.7 CYBER-CRIME INCIDENT MANAGEMENT PLAN

The incident management plan consists of four main stages:

- Containment and recovery to include investigating the breach and utilising appropriate staff to mitigate damage and recover any data lost where possible.
- Assessment of the ongoing risk to include confirming what data has been affected, what happened, whether relevant data was protected and how sensitive it is and identifying any other consequences of the breach/attack.
- Notification to consider if the cyber-attack needs to be reported to regulators (for example the ICO) and/or colleagues/parents as appropriate.
- Evaluation and response to consider any improvements to data security and evaluate future threats to security.

Where it is apparent that a cyber security incident involves a personal data breach, the Trust will invoke their Data Breach Policy rather than follow out the process in this section.

06. BIOMETRICS POLICY

6.1 WHAT IS BIOMETRIC DATA?

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

All biometric data is considered to be special category data under the UK General Data Protection Regulation (UK GDPR). This means the data is more sensitive and requires more protection and this type of data could create more significant risks to a person's fundamental rights and freedoms.

This policy complies with The Protection of Freedoms Act 2012 (sections 26 to 28), the Data Protection Act 2018 and the UK GDPR.

6.2 WHAT IS AN AUTOMATED BIOMETRIC RECOGNITION SYSTEM?

An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

6.3 THE LEGAL REQUIREMENTS UNDER UK GDPR.

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it.

As biometric data is special category data in order to lawfully process this data, the Trust must have a legal basis for processing personal data and a separate condition for processing special category data. When processing biometric data, the Trust rely on explicit consent (which satisfies the fair processing conditions for personal data and special category data).

6.4 CONSENT AND WITHDRAWAL OF CONSENT

The Trust will not process biometric information without the relevant consent.

6.5 CONSENT FOR PUPILS

When obtaining consent for pupils, both parents will be notified that the Trust intend to use and process their child's biometric information. The Trust only require written consent from one parent (in accordance with the Protection of Freedoms Act 2012), provided no parent objects to the processing.

If a parent objects to the processing, then the Trust will not be permitted to use that child's biometric data and alternatives will be provided.

The child may also object to the processing of their biometric data. If a child objects, the Trust will not process or continue to process their biometric data, irrespective of whether

consent has been provided by the parent(s).

Where there is an objection, the Trust will provide reasonable alternatives which will allow the child to access the same facilities that they would have had access to had their biometrics been used.

Pupils and parents can also object at a later stage to the use of their child's/their biometric data. Should a parent wish to withdraw their consent, they can do so by writing to the Trust at admin@theboleyntrust.org requesting that the Trust no longer use their child's biometric data.

Pupils who wish for the Trust to stop using their biometric data do not have to put this in writing but should let the schools Headteacher know.

The consent will last for the time period that your child attends the Trust (unless it is withdrawn).

6.6 CONSENT FOR STAFF

The Trust will seek consent of staff before processing their biometric data. If the staff member objects, the Trust will not process or continue to process the biometric data and will provide reasonable alternatives. Staff who wish for the Trust to stop using their biometric data should do so by writing to their Headteacher.

The consent will last for the time period that the staff member remains employed by the Trust (unless it is withdrawn).

6.7 RETENTION OF BIOMETRIC DATA

Biometric data will be stored by the Trust for as long as consent is provided (and not withdrawn).

Once a pupil [or staff member] leaves, the biometric data will be deleted from the Trust's system no later than 72 hours.

At the point that consent is withdrawn, the Trust will take steps to delete their biometric data from the system and no later than 72 hours.

6.8 STORAGE OF BIOMETRIC DATA

Biometric data will be kept securely and systems will be put in place to prevent any unauthorised or unlawful access/use.

The biometric data is only used for the purposes for which it was obtained and such data will not be unlawfully disclosed to third parties.

07. CCTV POLICY

7.1 INTRODUCTION

The Trust recognises that CCTV systems can be privacy intrusive.

For this reason, the Trust has carried out a data protection impact assessment with a view to evaluating whether the CCTV system in place is a necessary and proportionate means of achieving the legitimate objectives set out below.

The result of the data protection impact assessment has informed the Trust's use of CCTV and the contents of this policy.

Review of this policy shall be repeated regularly, and whenever new equipment is introduced a review will be conducted and a risk assessment put in place. We aim to conduct reviews no later than every two years.

7.2 OBJECTIVES

The purpose of the CCTV system is to assist the Trust in reaching these objectives:

(a) To protect pupils, staff and visitors against harm to their person and/or property.
(b) To increase a sense of personal safety and reduce the fear of crime.
(c) To protect the Trust buildings and assets.
(d) To support the police in preventing and detecting crime.
(e) To assist in identifying, apprehending and prosecuting offenders.
(f) To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence
(g) To assist in managing the Trust.

7.3 PURPOSE OF THIS POLICY

The purpose of this Policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at the Trust. The CCTV system used by the Trust can be obtained from the school.

7.4 STATEMENT OF INTENT

Notification has been submitted to the Information Commissioner and the next renewal date has been recorded.

The CCTV system will seek to comply with the requirements both of the Data Protection Act and the most recent Commissioner's Code of Practice.

The Trust will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial

purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site and make clear who is responsible for the equipment.

Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.

Recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated. In the absence of compelling a need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than agreed with the DPO.

7.5 SYSTEM MANAGEMENT

Access to the CCTV system and data shall be password protected.

The CCTV system will be administered and managed by the schools Headteacher who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager the system will be managed by the Head of ICT and Data Secuirty.

The system and the data collected will only be available to the Systems Manager, his/her replacement and appropriate members of the senior leadership team as determined by the Headteacher.

The CCTV system is designed to be in operation 24 hours each day, every day of the year, though the Trust does not guarantee that it will be working during these hours.

The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.

Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by proving clear, usable images.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those mentioned in above, requests access to the CCTV data or system, the System Manager must satisfy him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists access will be refused. Details of all visits and visitors will be recorded in a system log book including time/data of

access and details of images viewed and the purpose for so doing.

7.6 DOWNLOADING CAPTURED DATA ONTO OTHER MEDIA

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures:

(a) Each downloaded media must be identified by a unique mark.
(b) Before use, each downloaded media must be cleaned of any previous recording.
(c) The System Manager will register the date and time of downloaded media insertion, including its reference.
(d) Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a downloaded media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.
(e) If downloaded media is archived the reference must be noted.

Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his/her replacement and other authorised senior leaders as agreed by the Chief Finance and Operating Officer. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable if possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of the Trust, and downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The Trust also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the Trust to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until they are needed by the police.

Applications received from outside bodies (e.g. solicitors or parents) to view or release images will be referred to the Trust's Data Protection Officer and a decision made by the Chief Finance and Operating Officer and or the Chief Executive of the Trust in consultation with the Trust's data protection officer.

7.7 COMPLAINTS ABOUT THE USE OF CCTV

Any complaints in relation to the Trust's CCTV system should be addressed to the Headteacher in the first instance.

7.8 REQUEST FOR ACCESS BY THE DATA SUBJECT

The Data Protection Act provides Data Subjects – those whose image has been captured by the CCTV system and can be identified - with a right to access data held about themselves, including those obtained by CCTV. Requests for such data should be made to the school.

08. ELECTRONIC INFORMATION & COMMUNICATIONS SYSTEMS POLICY

8.1 INTRODUCTION

The Trust's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff at the Trust who are required to familiarise themselves and comply with its contents. The Trust reserves the right to amend its content at any time.

This policy outlines the standards that the Trust requires all users of these systems to observe, the circumstances in which the Trust will monitor use of these systems and the action the Trust will take in respect of any breaches of these standards.

The use by staff and monitoring by the Trust of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the UK General Data Protection Regulation (UK GDPR) and all data protection laws and guidance in force.

Staff are referred to the Trust's Data Protection Policy for further information. The Trust is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the Trust's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the Trust's disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

The Trust has the right to monitor all aspects of its systems, including data which is stored under the Trust's computer systems in compliance with the UK GDPR.

This policy mainly deals with the use (or misuse) of computer equipment, e-mail, internet connection, telephones, iPads (and other mobile device tablets), Blackberries, personal digital assistants (PDAs) and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and the like.

8.2 EQUIPMENT SECURITY AND PASSWORDS

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

Passwords are unique to each user and staff are required to select a password that cannot be easily broken and which contains at least 6 characters including both numbers and letters.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Group who will liaise with the Head of ICT and Data Security as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the Trust's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If given access to the Trust e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Group and/or the Head of ICT and Data Security may do spot checks from time to time to ensure compliance with this requirement.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the Trust's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Logging off prevents another member of staff accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that he or she was not the party responsible.

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of the Headteacher or Head of ICT and Data Security.

On the termination of employment for any reason, staff are required to provide a full handover detailing the drives, folders and files where their work can be located and accessed. The Trust reserves the right to require employees to hand over all Trust data held in computer useable format.

Members of staff who have been issued with a laptop, iPad (or other mobile device tablet), PDA or Blackberry must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers.

8.3 SYSTEMS USE AND DATA SECURITY

Members of staff should not delete, destroy or modify any of the Trust's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the Trust's, its staff, students, or any other party.

All members of staff are prohibited from downloading, installing or running software from external sources without submitting a request to the Head of ICT and Data Security and obtaining prior authorisation from the Chief Finance and Operating Officer who will

consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

Where consent is given all files and data should always be virus checked before they are downloaded onto the Trust's systems. If in doubt, the employee should seek advice from the Head of ICT and Data Security or a member of the Senior Leadership Group.

The following must never be accessed from the network because of their potential to overload the system or to introduce viruses:

- Audio and video streaming.
- Instant messaging.
- Chat rooms.
- Social networking sites.
- Web mail (such as Hotmail or Yahoo).

No device or equipment should be attached to our systems without the prior approval of the Head of ICT and Data Security. This includes, but is not limited to, any PDA or telephone, iPad (or other mobile device tablet), USB device, i-pod, digital camera, MP3 player, infra-red connection device or any other device.

The Trust monitors all e-mails passing through its systems for viruses. Staff should be cautious when opening e-mails from unknown external sources or where for any reason an e-mail appears suspicious (such as ending in '.exe'). The Head of ICT and Data Security should be informed immediately if a suspected virus is received. The Trust reserves the right to block access to attachments to e-mail for the purpose of effective use of the system and compliance with this policy. The Trust also reserves the right not to transmit any e-mail message.

Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of the Trust's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled Inappropriate Use of the Trust's Systems and guidance under "E-mail etiquette and content" below.

8.4 E-MAIL ETIQUETTE AND CONTENT

E-mail is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline.

The Trust's e-mail facility is intended to promote effective communication within the business on matters relating to the Trust's business activities and access to the Trust's e-mail facility is provided for work purposes only.

Staff are strictly prohibited from using the Trust's email facility for personal emails at any time.

Staff should always consider if e-mail is the appropriate medium for a particular

communication. The Trust encourages all members of staff to make direct contact with individuals rather than communicate by e-mail wherever possible to maintain and enhance good working relationships.

Messages sent on the e-mail system should be written as professionally as a letter or fax message and should be concise and directed only to relevant individuals on a need to know basis. The content and language used in the message must be consistent with the Trust's best practice.

E-mails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received. Staff are encouraged wherever practicable to write a draft e-mail first, print it out and review it carefully before finalising and sending. As a rule of thumb if a member of staff would not be happy for the e-mail to be read out in public or subjected to scrutiny then it should not be sent. Hard copies of e-mails should be retained on the appropriate file.

All members of staff should remember that e-mails can be the subject of legal action for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and the Trust. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the Trust in the same way as the contents of letters or faxes.

E-mail messages may of course be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail is obliterated and all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether e-mail is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

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

Staff should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling or working out of the office and should use an out of office response when away from the office for more than a day. Staff should endeavour to respond to e-mails marked 'high priority' as soon as is reasonably practicable.

Members of staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Group immediately. If a recipient asks you to stop sending them personal messages then always stop immediately. Where appropriate, the sender of the e-mail should be referred to this policy and asked to stop sending such material.

If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via e-mail, you should inform your Headteacher or Chief Finance and Operating Officer who will usually seek to resolve the matter informally.

If an informal procedure is unsuccessful, you may pursue the matter formally under the Trust's formal grievance procedure.

As general guidance, staff must not:

- Send any e-mail, including resending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally.
- Send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice.
- Send or forward private e-mails at work which they would not want a third party to read.
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the Trust.
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them.
- Sell or advertise using the systems or broadcast messages about lost property, sponsorship or charitable appeals.
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter.
- Download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this.
- Send messages containing any reference to other individuals or any other business that may be construed as libellous.
- Send messages from another worker's computer or under an assumed name unless specifically authorised.
- Send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.

E-mail may normally only be used to communicate internally with colleagues and students (where appropriate and necessary) and externally to parents, suppliers and third parties on academic/service related issues. Urgent or important messages to family and friends are permitted, but must be of a serious nature.

The Trust recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once. Any member of staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated.

Staff who receive an e-mail which has been wrongly delivered should return it to the sender of the message. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or forwarded to another member of staff or used in any way. The Head of ICT and Data Security should be informed as soon as reasonably practicable.

8.5 USE OF THE WEB AND INTERNET

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 an inappropriate one such a marker could be a source of embarrassment to the Trust, especially if a member of staff has accessed, downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if, for example, the material is pornographic in nature.

Staff must not therefore access from the Trust's system any web page or any files (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within the Trust (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the Trust's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

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

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

The Trust's website may be found at www.theboleyntrust.org.

The Trust has published relevant information on its own intranet for the use of all staff. All such information is regarded as confidential to the Trust and may not be reproduced electronically or otherwise for the purposes of passing it to any individual not directly employed by the Trust. Any exceptions to this must be authorised by the Chief Finance and Operating Officer or Chief Executive.

8.6 PERSONAL USE OF THE TRUST'S SYSTEMS

The Trust permits the incidental use of its internet, e-mail and telephone systems to send personal e-mail, browse the web and make personal telephone calls subject to certain conditions set out below.

Our policy on personal use is a privilege and not a right. The policy is dependent upon it not being abused or overused and we reserve the right to withdraw our permission or amend the scope of this policy at any time.

Staff are strictly prohibited from personal use of the Trust's systems.

Staff should be aware that any personal use of the systems may also be monitored (see below) and, where breaches of this policy are found, action may be taken under our Disciplinary Policy and Procedure. Any personal use of the Trust's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary

dismissal depending on the seriousness of the offence.

The Trust reserves the right to restrict or prevent access to certain telephone numbers or internet sites.

8.7 INAPPROPRIATE USE OF EQUIPMENT AND SYSTEMS

Access is granted to the web, telephones and to other electronic systems, for legitimate work purposes only.

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the Trust's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

(a) Accessing pornographic material (that is writings, pictures, and films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials.
(b) Transmitting a false and/or defamatory statement about any person or organisation.
(c) Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others.
(d) Transmitting confidential information about the Trust and any of its staff, students or associated third parties.
(e) Transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the Trust.
(f) Downloading or disseminating material in breach of copyright.
(g) Copying, downloading, storing or running any software without the express prior authorisation of the Head of ICT and Data Security.
(h) Engaging in on line chat rooms, instant messaging, and social networking sites and on line gambling.
(i) Forwarding electronic chain letters and other materials.
(j) Accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the Trust may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary such information may be handed to the police in connection with a criminal investigation.

09. COOKIE POLICY

9.1 INTRODUCTION

We ask that you read this cookie policy carefully as it contains important information on and our use of cookies on our website.

9.2 WHAT ARE COOKIES?

Cookies are small data files that are placed on your computer or mobile device when you visit a website. Cookies are widely used by online service providers to help build a profile of users. Some of this data will be aggregated or statistical, which means that we will not be able to identify you individually.

You can set your browser not to accept cookies. However, some of our website features may not function as a result.

9.3 TYPES OF COOKIES

The cookies we place on your device fall into the following categories:

- Session cookies—these allow our website to link your actions during a particular browser session. These expire each time you close your browser and do not remain on your device afterwards.
- Persistent cookies—these are stored on your device in between browser sessions. These allow your preferences or actions across our website to be remembered. These will remain on your device until they expire, or you delete them from your cache.
- Strictly necessary cookies—these cookies are essential for you to be able to navigate our website and use its features. Without these cookies, the services you have asked for could not be provided.
- Performance cookies—these cookies collect information about how you use our website, e.g. which pages you go to most often. These cookies do not collect personally identifiable information about you. All information collected by these cookies is aggregated and anonymous, and is only used to improve how our website works.
- Functionality cookies—these cookies allow our website to remember the choices you make (such as your user name, language, last action and search preferences) and provide enhanced, more personal features. The information collected by these cookies is anonymous and cannot track your browsing activity on other websites.
- Targeting cookies—also known as advertising cookies, these cookies are used to deliver adverts more relevant to you and your interests. They are also used to limit the number of times you see an advertisement on our website and help measure the effectiveness of the advertising campaign. They are usually placed by advertising networks with the website operator's permission. They remember that you have visited a website and this information is shared with other organisations such as advertisers.

9.4 HOW WE USE YOUR COOKIES

The Boleyn Trust may request cookies to be set on your computer or device. Cookies are

used to let us know when you visit our website, how you interact with us and to make your experience using the Trust website better for you. The cookies we collect will differ depending on what you are looking at on our website. You are able to adapt your cookie preferences, but by blocking certain types of cookie it may mean that your experience on the website is impacted.

9.5 CONSENT TO USE COOKIES

We will ask for your permission (consent) to place cookies or other similar technologies on your device, except where these are essential for us to provide you with a service that you have requested (e.g. to enable you to put items in your shopping basket and use our check-out process).

There is a notice on our home page which describes how we use cookies and requests your consent to place cookies on your device.

9.6 HOW TO TURN OFF COOKIES

If you do not want to accept cookies, you can change your browser settings so that cookies are not accepted. If you do this, please be aware that you may lose some of the functionality of this website. For further information about cookies and how to disable them please go to the Information Commissioner's webpage on cookies: https://ico.org.uk/for-the-public/online/cookies/.

10. DATA RETENTION POLICY

10.1 INTRODUCTION

The Trust has a responsibility to maintain its records and record keeping systems. When doing this, the Trust will take account of the following factors:

- The most efficient and effective way of storing records and information.
- The confidential nature of the records and information stored.
- The security of the record systems used.
- Privacy and disclosure.
- Their accessibility.

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the Trust's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the Trust from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect. The Trust may also vary any parts of this procedure, including any time limits, as appropriate in any case.

10.2 DATA PROTECTION

This policy sets out how long employment-related and pupil data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the UK General Data Protection Regulation (UK GDPR) and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the Trust. The Trust's Data Protection Policy outlines its duties and obligations under the UK GDPR.

10.3 RETENTION SCHEDULE

Information (hard copy and electronic) will be retained for at least the period specified in the Trusts retention schedule which can be obtained from the school. When managing records, the Trust will adhere to the standard retention times listed within that schedule.

The schedule is a relatively lengthy document listing the many types of records used by the Trust and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

10.4 DESTRUCTION OF RECORDS

Where records have been identified for destruction they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

All paper records containing personal information, or sensitive policy information should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate waste paper merchant. All electronic information will be deleted.

The Trust maintains a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record in this list at least:

- File reference (or other unique identifier).
- File title/description.
- Number of files.
- Name of the authorising Officer.
- Date destroyed or deleted from system.
- Person(s) who undertook destruction.

10.5 RECORD KEEPING OF SAFEGUARDING

Any allegations made that are found to be malicious must not be part of the personnel records.

For any other allegations made, the Trust must keep a comprehensive summary of the allegation made, details of how the investigation was looked into and resolved and any decisions reached. This should be kept on the personnel files of the accused.

Any allegations made of sexual abuse should be preserved by the Trust for the term of an inquiry by the Independent Inquiry into Child Sexual Abuse. All other records (for example, the personnel file of the accused) should be retained until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer. Guidance from the Independent Inquiry Child Sexual Abuse states that prolonged retention of personal data at the request of an Inquiry would not contravene data protection regulation provided the information is restricted to that necessary to fulfil potential legal duties that a Trust may have in relation to an Inquiry.

Whilst the Independent Inquiry into Child Sexual Abuse is ongoing, it is an offence to destroy any records relating to it. At the conclusion of the Inquiry, it is likely that an indication regarding the appropriate retention periods of the records will be made.

10.6 ARCHIVING

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by the Chief Finance and Operating Officer. The appropriate staff member, when archiving documents should record in this list the following information:

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

10.7 TRANSFERRING INFORMATION TO OTHER MEDIA

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate

data where necessary should always be considered.

10.8 TRANSFERRING INFORMATION TO ANOTHER TRUST OR SCHOOL

We retain the Pupil's educational record whilst the child remains at the Trust. Once a pupil leaves the Trust, the file should be sent to their next School. The responsibility for retention then shifts onto the next school or Trust. We retain the file for a year following transfer in case any issues arise as a result of the transfer.

We may delay destruction for a further period where there are special factors such as potential litigation.

10.9 RESPONSIBILITY AND MONITORING

The Headteacher has primary and day-to-day responsibility for implementing this Policy. The Data Protection Officer, in conjunction with the Trust is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The Data Protection Officer will consider the suitability and adequacy of this policy and report improvements directly to management.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.

Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this Policy and are given adequate and regular training on it.

10.10 EMAILS

Emails accounts are not a case management tool in itself. Generally emails may need to fall under different retention periods (for example, an email regarding a health and safety report will be subject to a different time frame to an email which forms part of a pupil record). It is important to note that the retention period will depend on the content of the email and it is important that staff file those emails in the relevant areas to avoid the data becoming lost.

10.11 PUPIL RECORDS

All Trusts with the exception of independent Trusts, are under a duty to maintain a pupil record for each pupil. Early Years will have their own separate record keeping requirements. If a child changes Trusts, the responsibility for maintaining the pupil record moves to the next Trust. We retain the file for a year following transfer in case any issues arise as a result of the transfer.

10.12 An up-to-date copy of the Trust's retention schedule can be obtained from the Chief Finance and Operating Officer.

11. SUBJECT ACCESS REQUEST POLICY

11.1 INTRODUCTION

The Trust holds personal data (or information) about job applicants, employees, pupils and parents and other individuals for a variety of purposes.

Under Data Protection Law, individuals (known as 'data subjects') have a general right to find out whether the Trust hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that the Trust are undertaking.

This policy provides guidance for staff members on how data subject access requests should be handled, and for all individuals on how to make a SAR.

Failure to comply with the right of access under the UK GDPR puts both staff and the Trust at potentially significant risk, and so the Trust takes compliance with this policy very seriously.

If you have any questions regarding this policy, please contact the Trust's DPO whose details are as follows:

Data Protection Officer:	Craig Stilwell
Address:	Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE
Email:	dataservices@judicium.com
Telephone:	0203 326 9174

11.2 DEFINITIONS

Data Subjects for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information

Personal Data means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties

11.3 HOW TO RECOGNISE A SUBJECT ACCESS REQUEST

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g. a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the Trust process personal data about him or her and, if so for access to that personal data and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text) or verbally (e.g. during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of all the information that you have about me' will be a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data, and not to information relating to other people.

11.4 HOW TO MAKE A DATA SUBJECT ACCESS REQUEST

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to use the Trust's form, which can be obtained from the school office. This allows the Trust to easily recognise that you wish to make a data subject access request.

11.5 WHAT TO DO WHEN YOU RECEIVE A DATA SUBJECT ACCESS REQUEST

All data subject access requests should be immediately directed to the Headteacher or Data Protection Champion who will contact the DPO for assistance if needed. There are limited timescales within which the Trust must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual. So it is crucial to ensure that requests are passed to the relevant individual without delay and failure to do so may result in disciplinary action being taken.

11..6 ACKNOWLEDGING THE REQUEST

When receiving a SAR the Trust shall acknowledge the request as soon as possible and inform the requester about the statutory deadline to respond to the request. In addition to acknowledging the request, the Trust may ask for proof of ID if needed or clarification about the requested information. If it is not clear where the information shall be sent, the Trust must clarify what address/email address to use when sending the requested information.

11.7 VERIFYING THE IDENTITY OF A REQUESTER OR REQUESTING CLARIFICATION OF THE REQUEST

Before responding to a SAR, the Trust will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The Trust is entitled to request additional information from a requester in

order to verify whether the requester is in fact who they say they are. Where the Trust has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the Trust may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The Trust shall let the requestor know as soon as possible that more information is needed before responding to the request.

In both cases, the period of responding begins when the additional information has been received. If the Trust do not receive this information, they will be unable to comply with the request.

11.8 FEE FOR RESPONDING TO A SUBJECT ACCESS REQUEST

The Trust will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the Trust will inform the requester why this is considered to be the case and that the Trust will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

11.9 TIME PERIOD FOR RESPONDING TO A SUBJECT ACCESS REQUEST

The Trust has one calendar month to respond to a SAR. This will run from the day the request has been received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

In circumstances where the Trust is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity, and in the case of a third party requester, the written authorisation of the data subject has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the Trust will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

11.10 TRUST CLOSURE PERIODS

Requests received during or just before Trust closure periods will not be able to be responded to within the one calendar month response period. This is because the Trust will be closed and no one will be on site to comply with the request. As a result, it is unlikely that your request will be received during this time (and so the time period does not run until we receive the request). We may not be able to acknowledge your request during this time (i.e. until a time we receive the request) and the time period may not start until the Trust re-opens. The Trust will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

11.12 INFORMATION TO BE PROVIDED IN RESPONSE TO A REQUEST

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- The purposes for which we process the data.
- The recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations.
- Where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period.
- The fact that the individual has the right to request that the Company rectifies, erases or restricts the processing of his personal data; or to object to its processing.
- To lodge a complaint with the ICO.
- Where the personal data has not been collected from the individual, any information available regarding the source of the data.
- Any automated decision we have taken about him or her, together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly-used electronic format.

The information that the Trust are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the Trust have one month in which to respond the Trust is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

The Trust is therefore, allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The Trust is not allowed to amend or delete data to avoid supplying the data.

11.13 HOW TO LOCATE INFORMATION

The personal data the Trust need to provide in response to a data subject access request

may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the Trust may need to search all or some of the following:

- Electronic systems, e.g. databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV.
- Manual filing systems in which personal data is accessible according to specific criteria, e.g. chronologically ordered sets of manual records containing personal data.
- Data systems held externally by our data processors [e.g. external payroll service providers].
- Occupational health records held by the [Occupational Health Department].
- Pension's data held by Teachers' Pension and Local Government Pension Scheme.
- Share scheme information.
- Insurance benefit information.
- Data held by third party consultants, e.g. outsourced HR professionals.

The Trust should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

11.14 REQUESTS MADE BY THIRD PARTIES

The Trust need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The Trust may also require proof of identity in certain circumstances.

If the Trust is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

11.15 REQUESTS MADE ON BEHALF OF CHILDREN

Even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the Trust should consider whether the child is mature enough to understand their rights. If the Trust is confident that the child can understand their rights, then the Trust should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- The child's level of maturity and their ability to make decisions like this.
- The nature of the personal data.
- Any court orders relating to parental access or responsibility that may apply.
- Any duty of confidence owed to the child or young person.
- Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment.
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information.
- Any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the Trust is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the Trust will require the written authorisation of the child before responding to the requester, or provide the personal data directly to the child.

The Trust may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example if it is likely to cause detriment to the child.

11.16 PROTECTION OF THIRD PARTIES - EXEMPTIONS TO THE RIGHT OF SUBJECT ACCESS

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The Trust will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the Trust do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individuals consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose.
- any duty of confidentiality they owe to the other individual.
- any steps taken to seek consent from the other individual.
- whether the other individual is capable of giving consent.
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the Trust disclosing the information

about them, then it would be unreasonable not to do so. However, if there is no such consent, the Trust must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

11.17 OTHER EXEMPTIONS TO THE RIGHT OF SUBJECT ACCESS

In certain circumstances the Trust may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The Trust do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The Trust do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- Education, training or employment of the individual.
- Appointment of the individual to any office.
- Provision by the individual of any service.

This exemption does not apply to confidential references that the Trust receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference), which means that the Trust must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The Trust do not have to disclose any personal data which are subject to legal professional privilege.

Management forecasting: The Trust do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The Trust do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

11.18 REFUSING TO RESPOND TO A REQUEST

The Trust can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If a request is found to be manifestly unfounded or excessive the Trust can:

- Request a "reasonable fee" to deal with the request; or
- Refuse to deal with the request.

In either case the Trust need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the Trust should contact the individual promptly and inform them. The Trust do not need to comply with the request until the fee has been received.

11.19 RECORD KEEPING

A record of all subject access requests shall be kept by the school. The record shall include the date the SAR was received, the name of the requester, what data the Trust sent to the requester and the date of the response.

12. FREEDOM OF INFORMATION POLICY & PUBLICATION SCHEME

12.1 INTRODUCTION

The Freedom of Information Act 2000 gives individuals the right to access official information from public bodies. Under the Act, any person has a legal right to ask for access to information held by the Trust. They are entitled to be told whether the Trust holds the information, and to receive a copy, subject to certain exemptions. While the Act assumes openness, it recognises that certain information is sensitive. There are exemptions to protect this information. Full details on how requests can be made are set out in section 1 of this policy.

Public Authorities should be clear and proactive about the information they will make public. For this reason, a publication scheme is available and can be found at section 2 of this policy.

This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect.

This policy should be used in conjunction with the Trust's Data Protection Policy.

12.2 FREEDOM OF INFORMATION REQUESTS

Requests under Freedom of Information should be made to the Headteacher. However, the request can be addressed to anyone in the Trust; so all staff need to be aware of the process for dealing with requests. Any member of staff receiving a request should pass this over to the Headteacher or Data Protection Champion.

Requests for information that are not data protection or environmental information requests will be covered by the Freedom of Information Act.

Data Protection enquiries (or Subject Access Requests/SARs) are requests where the enquirer asks to see what personal information the Trust holds about the enquirer. If the enquiry is a Data Protection request, the Trust's Data Protection Policy should be followed.

Environmental Information Regulations enquiries are those which relate to air, water, land, natural sites, built environment, flora and fauna, health, and any decisions and activities affecting any of these. These could, therefore, include enquiries about recycling, phone masts, Trust playing fields, car parking etc. If the enquiry is about environmental information, follow the guidance on the Department for Environment, Food and Rural Affairs (DEFRA) website.

Freedom of Information requests must be made in writing, (including email), and should include the enquirer's name, correspondence address (email addresses are allowed), and state what information they require. There must be enough information in the request to be able to identify and locate the information. If this information is covered by one of the other pieces of legislation (as referred to above), they will be dealt with under the relevant policy/procedure related to that request.

If the request is ambiguous and/or the Trust require further information in order to deal with your request, the Trust will request this further information directly from the

individual making the request. Please note that the Trust do not have to deal with the request until the further information is received. Therefore, the time limit starts from the date that the Trust receives all information required in order to deal with the request.

The requester does not have to mention the Act, nor do they have to say why they want the information. There is a duty to respond to all requests, telling the enquirer whether or not the information is held, and supplying any information that is held, except where exemptions apply. There is a time limit of 20 Trust days (i.e. excluding Trust holidays) for responding to the request.

Provided all requirements are met for a valid request to be made, the Trust will provide the information that it holds (unless an exemption applies).

Holding information means information relating to the business of the Trust:

- That the Trust has created; or
- That the Trust has received from another body or person; or
- Held by another body on the Trust's behalf.

Information means both hard copy and digital information, including email.

If the information is held by another public authority, such as the Local Authority, first check with them they hold it, then transfer the request to them. If this applies, the Trust will notify the enquirer that they do not hold the information and to whom they have transferred the request. The Trust will continue to answer any parts of the enquiry in respect of information it does hold.

When the Trust does not hold the information, it has no duty to create or acquire it just to answer the enquiry; although a reasonable search will be made before confirming whether the Trust has the information requested.

If the information requested is already in the public domain, for instance, through the Publication Scheme or on the Trust's website, the Trust will direct the enquirer to the information and explain how to access it.

The requester has the right to be told if the information requested is held by the Trust (subject to any of the exemptions). This obligation is known as the Trust's duty to confirm or deny that it holds the information. However, the Trust does not have to confirm or deny if:

- The exemption is an absolute exemption; or
- In the case of qualified exemptions, confirming or denying would itself disclose exempted information.

12.3 VEXATIOUS REQUESTS

There is no obligation on the Trust to comply with vexatious requests. A vexatious request is one which is designed to cause inconvenience, harassment or expense rather than to obtain information, and would require a substantial diversion of resources or would otherwise undermine the work of the Trust. However, this does not provide an excuse for bad records management.

In addition, the Trust do not have to comply with repeated identical or substantially similar requests from the same applicant unless a reasonable interval has elapsed between requests.

12.4 FEES

The Trust may charge the requester a fee for providing the requested information. This will be dependent on whether the staffing costs in complying with the request exceeds the threshold. The threshold is currently £450 with staff costs calculated at a fixed rate of £25 per hour (therefore 18 hours' work is required before the threshold is reached).

If a request would cost less than the threshold, then the Trust can only charge for the cost of informing the applicant whether the information is held, and communicating the information to the applicant (e.g. photocopying, printing and postage costs).

When calculating costs/threshold, the Trust can take account of the staff costs/time in determining whether the information is held by the Trust, locating and retrieving the information, and extracting the information from other documents. The Trust will not take account of the costs involved with considering whether information is exempt under the Act.

If a request would cost more than the appropriate limit, (£450) the Trust can turn the request down, answer and charge a fee or answer and waive the fee.

If the Trust are going to charge they will send the enquirer a fees notice. The Trust do not have to comply with the request until the fee has been paid. More details on fees can be found on the ICO website.

If planning to turn down a request for cost reasons, or charge a high fee, you should contact the applicant in advance to discuss whether they would prefer the scope of the request to be modified so that, for example, it would cost less than the appropriate limit.

Where two or more requests are made to the Trust by different people who appear to be acting together or as part of a campaign the estimated cost of complying with any of the requests may be taken to be the estimated total cost of complying with them all.

12.5 TIME LIMITS

Compliance with a request must be prompt and within the time limit of 20 Trust days (this does not include the Trust holidays or weekends) or 60 working days if this is shorter. Failure to comply could result in a complaint by the requester to the Information Commissioner's Office. The response time starts counting as the first day from the next working day after the request is received (so if a request was received on Monday 6th October the time limit would start from the next working day, the 7th October).

Where the Trust has asked the enquirer for more information to enable it to answer, the 20 Trust days start time begins when this further information has been received.

If some information is exempt this will be detailed in the Trust's response.

If a qualified exemption applies and the Trust need more time to consider the public

interest test, the Trust will reply in 20 Trust days stating that an exemption applies but include an estimate of the date by which a decision on the public interest test will be made. This should be within a "reasonable" time.

Where the Trust has notified the enquirer that a charge is to be made, the time period stops until payment is received.

12.6 THIRD PARTY DATA

Consultation of third parties may be required if their interests could be affected by release of the information requested, and any such consultation may influence the decision.

Consultation will be necessary where:

- Disclosure of information may affect the legal rights of a third party, such as the right to have certain information treated in confidence or rights under Article 8 of the European Convention on Human Rights;
- The views of the third party may assist the Trust to determine if information is exempt from disclosure; or
- The views of the third party may assist the Trust to determine the public interest test.

Personal information requested by third parties is also exempt under this policy where release of that information would breach the Data Protection Act. If a request is made for a document (e.g. Governing Body minutes) which contains personal information whose release to a third party would breach the Data Protection Act, the document may be issued by blanking out the relevant personal information as set out in the redaction procedure.

12.7 EXEMPTIONS

The presumption of the Freedom of Information Act is that the Trust will disclose information unless the Act provides a specific reason to withhold it. The Act recognises the need to preserve confidentiality and protect sensitive material in certain circumstances.

The Trust may refuse all/part of a request, if one of the following applies:

- There is an exemption to disclosure within the act.
- The information sought is not held.
- The request is considered vexatious or repeated; or
- The cost of compliance exceeds the threshold.

A series of exemptions are set out in the Act which allow the withholding of information in relation to an enquiry. Some are very specialised in their application (such as national security) and would not usually be relevant to Trusts.

There are two general categories of exemptions:

- Absolute: where there is no requirement to confirm or deny that the information is held, disclose the information or consider the public interest; and
- Qualified: where, even if an exemption applies, there is a duty to consider the public interest in disclosing information.

12.7.1 ABSOLUTE EXEMPTIONS

There are eight absolute exemptions set out in the Act. However the following are the only absolute exemptions which will apply to the Trust:

- Information accessible to the enquirer by other means (for example by way of the Trust's Publication Scheme);
- National Security/Court Records;
- Personal information (i.e. information which would be covered by the Data Protection Act);
- Information provided in confidence.

If an absolute exemption exists, it means that disclosure is not required by the Act. However, a decision could be taken to ignore the exemption and release the information taking into account all the facts of the case if it is felt necessary to do so.

12.7.2 QUALIFIED EXEMPTIONS

If one of the below exemptions apply (i.e. a qualified disclosure), there is also a duty to consider the public interest in confirming or denying that the information exists and in disclosing information.

The qualified exemptions under the Act which would be applicable to the Trust are:

- Information requested is intended for future publication (and it is reasonable in all the circumstances for the requester to wait until such time that the information is actually published);
- Reasons of National Security;
- Government/International Relations;
- Release of the information is likely to prejudice any actual or potential legal action or formal investigation involving the Trust;
- Law enforcement (i.e. if disclosure would prejudice the prevention or detection of crime, the prosecution of offenders or the administration of justice);
- Release of the information would prejudice the ability of the Trust to carry out an effective audit of its accounts, resources and functions;
- For Health and Safety purposes;
- Information requested is Environmental information;
- Information requested is subject to Legal professional privilege; and
- For Commercial Interest reasons.

Where the potential exemption is a qualified exemption, the Trust will consider the public interest test to identify if the public interest in applying the exemption outweighs the public interest in disclosing it.

In all cases, before writing to the enquirer, the person given responsibility by the Trust for dealing with the request will need to ensure that the case has been properly considered, and that the reasons for refusal, or public interest test refusal, are sound.

12.8 REFUSAL

If it is decided to refuse a request, the Trust will send a refusals notice, which must contain:

- The fact that the responsible person cannot provide the information asked for;
- Which exemption(s) apply;
- Why the exemption(s) apply to this enquiry (if it is not self-evident);
- Reasons for refusal; and
- The Trust's complaints procedure.

For monitoring purposes and in case of an appeal against a decision not to release the information or an investigation by the Information Commissioner, the responsible person must keep a record of all enquiries where all or part of the requested information is withheld and exemptions are claimed. The record must include the reasons for the decision to withhold the information.

12.9 FREEDOM OF INFORMATION PUBLICATION SCHEME

This publication scheme follows a model approved by the Information Commissioners Office.

This scheme is not a list of individual publications but rather a description of the classes of types of information that we are committed to publishing. This list is not an exhaustive list of all of the types of information that we publish. We try to proactively publish as much information as we can where the information would have a wider public interest.

This scheme does not include information that we consider to be sensitive, such as personal information, information prevented from disclosure by law or information about security matters.

12.9.1 CLASSES OF INFORMATION

There are six classes of information that we hold:

- Who we are and what we do
- What we spend and how we spend it
- What our priorities are and how we are doing
- How we make decisions
- Our policies and procedures
- The services we offer

12.9.2 MAKING INFORMATION AVAILABLE

Information will generally be made available on the Trust/school website. Where it is not possible to include this information on the Trust website, or when an individual does not wish to access the information by the website the Trust will indicate how information can be obtained by other means and provide it by those means. This may be detailed in response to a request or within the scheme itself. This will usually be by way of a paper copy.

In some exceptional circumstances, some information may be available only by

viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where we are legally required to translate any information, we shall do so.

12.9.3 CHARGES FOR INFORMATION PUBLISHED UNDER THE SCHEME

The Trust may charge individuals for information published under this scheme. The purpose of this scheme is to make the maximum amount of information readily available at the minimum inconvenience and cost to the public. Charges made by the Trust for routinely published material will be justified and transparent and kept to a minimum.

Material which is published and accessed on the website will be provided free of charge.

Charges may be made for information subject to a charging regime specified by law.

Charges will be made to cover:

- Photocopying;
- Postage and Packaging; &
- The costs directly incurred as a result of viewing information.

Single copies of information requested which are covered by the publication scheme will be provided free unless otherwise stated within the scheme. If the request involved a large amount of photocopying, printing or postage, then this may be at a cost. If this is the case we will let you know as well as let you know the cost before fulfilling your request.

12.9.4 HOW TO REQUEST INFORMATION

If you require a paper version of any of the documents within the scheme, please contact the Trust using the contact details below.

Contact:	Steven Lock
Telephone:	020 7476 1848
Email:	admin@theboleyntrust.org
Address:	The Boleyn Trust Tollgate Primary School Barclay Road London E13 8SA

Please mark all correspondence Publication Scheme Request in order to help us process your request quickly. If the information you are looking for isn't available via the scheme, you can still contact the Trust to ask if we have this information.

12.10 COMPLAINTS AND/OR APPEALS

Any written (including email) expression of dissatisfaction should be handled through the Trust's existing complaints procedure. Wherever practicable the review should be handled by someone not involved in the original decision.

The Governing Body should set and publish a target time for determining complaints and information on the success rate in meeting the target. The Trust should maintain records of all complaints and their outcome.

If the outcome is that the Trust's original decision or action is upheld, then the applicant can appeal to the Information Commissioner. The appeal can be made via their website or in writing to:

Customer Contact
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

13. HOME WORKING POLICY

13.1 INTRODUCTION

This policy applies to all staff who work from home and/or use or access Trust systems or information from home or while working remotely. This includes individuals who are given access to the Trust networks and Trust data (including governors, students, visitors, volunteers, contractors and third parties). It applies to information in all formats, including paper records and electronic data.

Remote working means working off the Trust site. This includes working while connected to the Trust's WiFi networks.

A mobile device is defined as a portable device which can be used to store or process information. Examples include but are not limited to laptops, tablets, USB sticks, removable disc drives and smartphones.

13.2 AWARENESS OF RISK

Working from home presents both significant risks and benefits.

Staff may have remote access to information held on secure Trust servers, but without the physical protections available in Trust and the network protections provided by firewalls and access controls there are much greater risks of unauthorised access to, and loss or destruction of, data. There are also greater risks posed by information "in transit" (i.e. moving data between office and home).

The risks posed by working from home can be summarised under three headings:

- Reputational: the loss of trust or damage to the Trust's relationship with its community.
- Personal: unauthorised loss of, or access to data could expose staff or students to identity theft, fraud or significant distress; and
- Monetary: regulators such as the ICO can impose financial penalties and those damaged as a consequence of a data breach may seek redress through the courts.

13.3 ROLES AND RESPONSIBILITIES

The decision as to whether to allow partial or full-time homeworking in relation to any given role rests with management.

Any member of staff working from home is responsible for ensuring that they work securely and protect both information and Trust-owned equipment from loss, damage or unauthorised access.

Managers are responsible for supporting their staff's adherence with this policy. Additional measures may be put in place by management to ensure the rules contained within this policy are adhered to (for example monitoring or supervision).

Failure to comply with this policy may result in disciplinary action.

13.4 KEY PRINCIPLES OF HOMEWORKING

Staff working from home must ensure that they work in a secure and authorised manner. This can be done by complying with the principles below:

- To adhere to the principles of the Data Protection Act 2018 and the Trust's Data Protection Policy in the same way as they would if they were working in Trust.
- Access to personal data must be controlled. This can be done through physical controls, such as locking the home office for physical data, and locking the computer by using strong passwords (a mixture of letters, numbers and special characters).
- No other members of the household should know or can guess your password(s). If passwords are written down (which should be a last case scenario) they must be stored securely (e.g. in a locked drawer or in a secure password protected database). Passwords should never be left on display for other to see.
- Automatic locks should be installed on IT equipment used to process Trust information that will activate after a period of inactivity (i.e. computers should automatically lock requiring you to sign back in after this period of time).
- IT equipment used to process and store Trust information in the home must be kept in a secure place where it cannot be easily accessed or stolen.
- Portable mobile devices used to process and store Trust information should be encrypted where possible (or at least password/pin code protected) and should never be left unattended in a public place.
- IT equipment in the home used to process Trust information should not be used where it can be overseen by unauthorised persons.
- It is the responsibility of each member of staff to ensure that they are working in a safe environment at home. No health and safety risks must be taken when using this equipment.
- Access to certain systems and services by those working from home or remotely may be deliberately restricted or may require additional authentication methods (such as two factor authentication using an additional device to verify individuals). Any attempt to bypass these restrictions may lead to disciplinary action.
- All personal information and in particular sensitive personal information should be encrypted/password protected before being sent by email where possible. Extra care must be taken when sending emails where auto-complete features are enabled (as this can lead to sending emails to similar/incorrect email addresses). The rules relating the sending of emails are outlined in the Trust's Acceptable Use Agreement.
- Always use your Trust email address when contacting colleagues or students. If telephoning a child or parent at their home ensure that your caller ID is blocked.
- Any technical problems (including, but not limited to, hardware failures and software errors) which may occur on the systems must be reported to the schools ICT Technician or Head of ICT and Data Security immediately.
- To adhere to the Trust's data retention policy and in particular ensure that information held remotely is managed according to the data retention schedule and securely deleted and destroyed once it is no longer needed.
- If communicating remotely via video conferencing and social media staff must adhere to using only those platforms which have been approved by the Trust and follow the Trust's guidance on the safe use of video conferencing.
- To be vigilant to phishing emails and not clicking on unsafe links. If clicked these links could lead to malware infection, loss of data or identity theft.

- Staff should not access inappropriate websites on Trust devices or whilst accessing Trust networks.

Staff who have been provided with Trust-owned IT equipment to work from home must:

- only use the equipment for legitimate work purposes;
- only install software on that equipment if authorised by the Trust's IT support. Please note that this includes screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins;
- ensure that the equipment is well cared for and secure;
- not allow non-staff members (including family, flatmates and friends) to use the equipment or to share log in passwords or access credentials with them;
- not attempt to plug in memory sticks into the equipment unless encrypted and supplied by the Trust);
- not collect or distribute illegal material via the internet;
- ensure anti-virus software is regularly updated; and
- to return the equipment securely at the end of the remote working arrangement.

Staff who process Trust data on their own equipment are responsible for the security of the data and the devices generally and must follow the Trust's Bring Your Own Device Policy and Acceptable Use Policy. In particular:

- Devices must be encrypted where possible;
- An appropriate passcode/password must be set for all accounts which give access to the device. Passwords must be complex (a mix of letters, numbers and special characters) and must not be shared with others;
- The device must be configured to automatically lock after a period of inactivity (no more than 15 minutes);
- Devices must remain up to date with security software (such as anti-virus software);
- The theft or loss of a device must be reported to IT services just in the same way as if a Trust-owned device were lost;
- Any use of privately-owned devices by others (family or friends) must be controlled in such a way as to ensure that they do not have access to Trust information. This will include Trust emails, learning platforms and administrative systems such as SIMs;
- Devices must not be left unattended where there is a significant risk to theft;
- The amount of personal data stored on the device should be restricted and the storing of any sensitive data avoided;
- Using open (unsecured) wireless networks should be avoided. Consider configuring your device not to connect automatically to unknown networks;
- If the device needs to be repaired, ensure that the company used is subject to a contractual agreement which guarantees the secure handling of any data stored on the device;
- Appropriate security must be obtained for all Trust information stored on the device (including back up arrangements) and there must be secure storage for any confidential information;
- Care must be taken with file storage. Any Trust related work should be stored on the Trust network area. No Trust data should be stored on a home computer or on an un-encrypted storage device (such as USB stick);

- The Trust may require access to a privately owned device when investigating policy breaches (for example to investigate cyber bullying);
- All data must be removed from privately-owned devices when it is no longer needed or at the request of the Trust; and
- Devices must be disposed of securely when no longer required.

Staff are responsible for ensuring the security of Trust property and all information, files, documents, data etc within their possession, including both paper and electronic material. In particular physical data (i.e. paper documents, which includes documents printed at home) must be secured and Staff must ensure that:

- Paper documents are not removed from the Trust without the prior permission of the Headteacher and or Chief Finance and Operating Officer. When such permission is given reasonable steps must be taken to ensure the confidentiality of the information is maintained during transit. In particular the information is not to be transported in see-through bags or other un-secured storage containers.
- Paper documents should not be used in public places and not left unattended in any place where it is at risk (e.g. in car boots, in a luggage rack on public transport);
- paper documents taken home or printed at home containing personal information, sensitive data and confidential information are not left around where they can be seen, accessed or removed;
- paper documents are collected from printers as soon as they are produced and not left where they can be casually read;
- the master copy of the data is not to be removed from Trust premises;
- Paper documents containing personal data are locked away in suitable facilities such as secure filing cabinets in the home just as they would be in Trust;
- documents containing confidential personal information are not pinned to noticeboards where other members of the household may be able to view them; and
- paper documents are disposed of securely by shredding and should not be disposed of with the ordinary waste unless it has been shredded first.

Any staff member provided with Trust devices must not do, cause or permit any act or omission which will avoid coverage under the Trust's insurance policy. If in any doubt as to whether particular acts or omissions will have this effect, the staff member should consult their line manager immediately.

All staff must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of any Trust-owned IT equipment or data immediately to the Head of ICT and Data Security who will promptly inform the Chief Finance and Operating Officer in order that appropriate steps may be taken quickly to protect Trust data. Failure to do so immediately may seriously compromise Trust security. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

13.5 HOMEWORKING GUIDANCE FOR STAFF

STOP working from home or remotely if you are handling high risk/sensitive data:

- On a device without adequate protection (antivirus, encryption)

- In a public space (café, train)
- On public/unsecured WiFi connection
- Without Trust authorisation

BEWARE

- Home printer-sharing, remote desktop file-sharing, remote USB connections
- Increased risk of hackers – This is not just about using devices or systems that are less secure, but also the risk of employees being duped into changing passwords or to download software that contains malware. Always be careful which websites you visit and which email attachments you open

CAUTION working from home or remotely

- Using personally owned devices (tablet, smartphone)
- Using unknown WiFi connections

OK to work from home or remotely

- whilst on Trust premises/servers
- using a Trust owned device
- using a Trust owned device which is directly connected to the Trust network
- using a device and/or data which is encrypted.

13.6 DISCLAIMER

Staff are expected to use Trust owned and privately owned devices in an ethical manner at all times and adhere to the Trust's policy as outlined above.

The Trust reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this policy.

The Trust reserves the right to disconnect devices or disable services or access to services without notification.

I confirm that I have read, understood and will comply with the terms of this Home Working Policy.

Signed: ……

Date: …….

Print Name: …….

14. BRING YOUR OWN DEVICE POLICY

14.1 INTRODUCTION

The Trust has implemented this policy to protect the Trust and all parties when using ICT and media devices. Staff are able to use devices at work and outside of work for work related activities provided the terms of this policy are met. The Trust reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of the Trust's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. This policy is not designed to offer protection for the device itself. The safety of the user's own device is the responsibility of the user.

Mobile devices within the context of this policy includes any mobile phone, tablet, laptop, MP3/iPod or other device which is capable of connecting with the internet or mobile networks or taking image or sound recordings.

This guidance is in addition to the Trust's Acceptable Use Policy.

All employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

14.2 ACCEPTABLE USE

The Trust embrace the use of new and mobile technologies and acknowledge they are a valuable resource in the classroom having educational purpose.

However by accessing the Trust's systems and networks, it is likely that staff will use personal data and so must abide by the terms of the Data Protection Act 2018 when doing (including ensuring adequate security of that personal information).

All staff who wish to use their own devices to access the Trust's network must sign and return the statement at the conclusion of this policy.

When in Trust staff should connect their device via the Trust's wireless network for security.

When out of Trust/School premises, staff should access work systems on their mobile device using "secure connections".

All internet access via the network is logged and, as set out in the Acceptable Use policy, employees are blocked from accessing certain websites whilst connected to the Trust network.

The use of camera, microphone and/or video capabilities are prohibited whilst on Trust premises unless this has been approved by the Headteacher and or the Chief Finance and Operating Officer. If approved, any pictures, videos or sound recordings can only be used for Trust purposes and cannot be posted or uploaded to any website or system outside of the Trust network.

You must not use your device to take pictures/video/recordings of other individuals without their advance written permission to do so.

14.3 NON-ACCEPTABLE USE

- Any apps or software that are downloaded onto the user's device whilst using the Trust's own network is done at the users risk and not with the approval of the Trust.
- Devices may not be used at any time to:
  - Store or transmit illicit materials;
  - Store or transmit proprietary information belonging to the Trust;
  - Harass others;
  - Act in any way against the Trust's acceptable use policy and other safeguarding and data related policies.
- Technical support is not provided by the Trust on the user's own devices

14.4 DEVICES AND SUPPORT

- Smartphones including iPhones and Android phones are allowed.
- Tablets including iPad and Android are allowed.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

14.5 SECURITY

In order to prevent unauthorised access, devices must be password/pin/fingerprint protected using the features of the device and a strong password is required to access the Trust network.

When using personal data, it is the user's responsibility to ensure they keep data secure on their device. This includes preventing theft and loss of data (for example through password protection and cloud back up) keeping information confidential (for example by ensuring access to emails or sensitive information is password protected) and maintaining that information.

The Trust does not accept responsibility for any loss or damage to the user's device when used on the Trust's premises. It is up to the user to ensure they have their own protection on their own device (such as insurance).

Staff are prevented from installing email apps which allow direct access to Trust emails without use of a login/password.

If information is particularly sensitive then users should ensure that the data is either appropriately secured or deleted from the device (including from any local copies which may have been stored on the device.

In the event of any loss or theft of personal data, this must be reported immediately as a data breach in accordance with the Trust's data breach policy.

The Trust may require access to a device when investigating policy breaches (for example to investigate cyber bullying).

Staff are not permitted to share access details to the Trust's network or Wi-Fi password with anyone else.

The Trust will not monitor the content of the user's own device but will monitor any traffic over the Trust system to prevent threats to the Trust's network.

14.6 DISCLAIMER

The Trust reserves the right to disconnect devices or disable services without notification. The employee is expected to use his or her devices in an ethical manner at all times and adhere to the Trust's policy as outlined above.

The employee is personally liable for all costs associated with his or her device.

The Trust reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this policy.

I confirm that I have read, understand and will comply with the terms of this Bring Your Own Device Policy when using my mobile device to access the Trust network

Signed: ……

Date: …….

Print Name: ……

15. SOCIAL MEDIA POLICY

15.1 INTRODUCTION

This policy applies to all Trust staff regardless of their employment status. It is to be read in conjunction with the Trust's Electronic Communications Policy. This policy does not form part of the terms and conditions of employee's employment with the Trust and is not intended to have contractual effect. It does however set out the Trust's current practices and required standards of conduct and all staff are required to comply with its contents. Breach of the provisions of this policy will be treated as a disciplinary offence which may result in disciplinary action up to and including summary dismissal in accordance with the Trust's Disciplinary Policy and Procedure.

This Policy may be amended from time to time and staff will be notified of any changes no later than one month from the date those changes are intended to take effect.

15.2 PURPOSE OF THIS POLICY

The Trust recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, LinkedIn, blogs and Wikipedia. However, staff use of social media can pose risks to the Trust's confidential and proprietary information, its reputation and it can jeopardise our compliance with our legal obligations

To minimise these risks, avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate work related purposes, all Trust staff are required to comply with the provisions in this policy.

15.3 WHO IS COVERED BY THIS POLICY?

This policy covers all individuals working at all levels and grades within the Trust, including senior managers, officers, governors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as Staff in this policy).

Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

15.4 SCOPE AND PURPOSE OF THIS POLICY

This policy deals with the use of all forms of social media including Facebook, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs.

It applies to the use of social media for both work and personal purposes, whether during work hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.

Breach of this policy may result in disciplinary action up to and including dismissal.

Disciplinary action may be taken regardless of whether the breach is committed during

working hours and regardless of whether the Trust's equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

15.5 PERSONNEL RESPONSIBLE FOR IMPLEMENTING THE POLICY

The Trust Board have overall responsibility for the effective operation of this policy, but have delegated day-to-day responsibility for its operation to the Chief Finance and Operating Officer and Headteachers.

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Headteacher in liaison with the IT Manager.

All senior Trust Staff have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All Trust Staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Headteacher in the first instance. Questions regarding the content or application of this policy should be directed by email to the Chief Finance and Operating Officer.

15.6 COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

- Breach our Electronic information and communications systems policy;
- Breach our obligations with respect to the rules of relevant regulatory bodies;
- Breach any obligations they may have relating to confidentiality;
- Breach our Disciplinary Rules;
- Defame or disparage the Trust, its Staff, its pupils or parents, its affiliates, partners, suppliers, vendors or other stakeholders;
- Harass or bully other Staff in any way or breach our Anti-harassment and bullying policy;
- Unlawfully discriminate against other Staff or third parties or breach our Equal opportunities policy;
- Breach our Data protection policy (for example, never disclose personal information about a colleague online);
- Breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the Trust

and create legal liability for both the author of the reference and the organisation.

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

15.7 PERSONAL USE OF SOCIAL MEDIA

Personal use of social media is never permitted during working time or by means of our computers, networks and other IT resources and communications systems.

Staff should not use a work email address to sign up to any social media and any personal social media page should not make reference to their employment with the Trust (excluding LinkedIn, where prior permission is sought from the Chief Finance and Operating Officer).

Staff must not take photos or posts from social media that belongs to the Trust for their own personal use.

15.8 MONITORING

The contents of our IT resources and communications systems are the Trust's property. 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 communications systems.

The Trust reserves the right to monitor, intercept and review, without further notice, Staff members activities using our 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 acknowledgement of this policy and 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.

The Trust may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

All Staff are advised not to use our IT resources and communications systems for any matter that he or she wishes to be kept private or confidential from the Trust.

15.9 EDUCATIONAL OR EXTRA CURRICULAR USE OF SOCIAL MEDIA

If your duties require you to speak on behalf of the Trust in a social media environment, you must follow the protocol outlined below.

The Trust may require you to undergo training before you use social media on behalf of the Trust and impose certain requirements and restrictions with regard to your activities.

Likewise, if you are contacted for comments about the Trust/School for publication

anywhere, including in any social media outlet, you must direct the inquiry to the Chief Finance and Operating Officer and or the Chief Executive and must not respond without advanced written approval.

15.10 RECRUITMENT

The Trust may use internet searches to perform pre employment checks on candidates in the course of recruitment. Where the Trust does this, it will act in accordance with its data protection and equal opportunities obligations.

15.11 RESPONSIBLE USE OF SOCIAL MEDIA

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

15.11.1 Photographs for use of Social Media

Any photos for social media posts may only be taken using Trust cameras/devices or devices that have been approved in advance by the Chief Finance and Operating Officer and or the Headteacher. Where any device is used that does not belong to the Trust all photos must be deleted immediately from the device, once the photos have been uploaded to a device belonging to the Trust.

15.11.2 Staff Protocol for use of Social Media

Where any post is going to be made on the Trust's own social media the following steps must be taken:

- Ensure that permission from the child's parent has been sought before information is used on social media (via [Parent/Social Media Agreement]).
- Ensure that there is no identifying information relating to a child/children in the post - for example any certificates in photos are blank/without names or the child's name cannot be seen on the piece of work.
- The post must be a positive and relevant post relating to the children, the good work of staff, the Trust or any achievements.
- Social Media can also be used to issue updates or reminders to parents/guardians and the Chief Finance and Operating Officer and Headteacher will have overall responsibility for this.
- The proposed post must be presented to the Chief Finance and Operating Officer (Trust) and or Headteacher (school) for confirmation that the post can 'go live' before it is posted on any social media site.
- The Headteacher or their nominated contact will post the information, but all staff have responsibility to ensure that the Social Media Policy has been adhered to.

15.11.3 Protecting our business reputation

Staff must not post disparaging or defamatory statements about:

- The Trust;
- Current, past or prospective Staff as defined in this policy

- Current, past or prospective pupils
- Parents, carers or families of pupils current, past or prospective
- The Trust's suppliers and services providers; and
- Other affiliates and stakeholders.

Staff should also avoid social media communications that might be misconstrued in a way that could damage the Trust's reputation, even indirectly.

If Staff are using social media they should make it clear in any social media postings that they are speaking on their own behalf. Staff should write in the first person and use a personal rather than Trust e-mail address when communicating via social media.

Staff are personally responsible for what they communicate in social media. Staff should remember that what they publish might be available to be read by the masses (including the Trust itself, future employers and social acquaintances) for a long time. Staff should keep this in mind before they post content.

If Staff disclose whether directly or indirectly their affiliation to the Trust as a member of Staff whether past, current or prospective, they must also state that their views do not represent those of the Trust.

Staff must ensure that their profile and any content posted are consistent with the professional image they are required to present to colleagues, pupils and parents.

Staff must avoid posting comments about confidential or sensitive Trust related topics. Even if Staff make it clear that their views on such topics do not represent those of the Trust, such comments could still damage the Trust's reputation and incur potential liability.

If a member of Staff is uncertain or concerned about the appropriateness of any statement or posting, he or she should refrain from making the communication until he or she has discussed it with their Line Manager.

If a member of Staff sees content in social media that disparages or reflects poorly on the Trust, it's Staff, pupils, parents, service providers or stakeholders, he or she is required to report this in the first instance to the Headteacher without unreasonable delay. **All staff are responsible for protecting the Trust's reputation**.

15.12 RESPECTING INTELLECTUAL PROPERTY AND CONFIDENTIAL INFORMATION

Staff should not do anything to jeopardise Trust confidential information and intellectual property through the use of social media.

In addition, Staff should avoid misappropriating or infringing the intellectual property of other Trust's, organisations, companies and individuals, which can create liability for the Trust, as well as the individual author.

Staff must not use the Trust's logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without express prior written permission from the Chief Finance and Operating Officer.

To protect yourself and the Trust against liability for copyright infringement, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Chief Finance and Operating Officer in the first instance before making the communication.

15.13 RESPECTING COLLEAGUES, PUPILS, PARENTS, CLIENTS, SERVICE PROVIDERS AND STAKEHOLDERS

Staff must not post anything that their colleagues, the Trust's past, current or prospective pupils, parents, service providers or stakeholders may find offensive, including discriminatory comments, insults or obscenity.

Staff must not post anything related to colleagues, the Trust's past, current or prospective pupils, parents, service providers or stakeholders without their advanced written permission.