Monitoring Procedure for The Beam Trust's Internet and Communications Facilities

Version	Date	Action
1	February 2023	Adopted by The Beam Trust from the LA
2		
3		

CONTENTS **PAGE**

1. INTRODUCTION

1.1 Internet, email and file storage facilities are the property of the Trust. All internet web use and emails are logged by the Trust School's.

1.2 Whilst the School's within the Trust do not currently undertake systematic monitoring, it reserves the right to do so at any time. Please refer to the Acceptable Use Policy for more information on monitoring and personal use.

1.3 Every attempt by a user to access a web-site is automatically logged and activities monitored.

1.4 Certain types of web site, such as those containing pornographic material, may not be accessed from school. A web accessing filtering system is in place that denies access to such sites. All attempts to access these banned sites are logged together with the log-in ID of the user, the time and date and the address of the website. This log is monitored in order to ensure that all users are complying with the Acceptable Use Policy. Repeated misuse will be reported to the Headteacher.

1.5 The Trust may, at its discretion, apply automatic message monitoring, filtering and rejection systems as appropriate and deny transmission of messages with content that is unacceptable in the terms of the Acceptable Use Policy.

1.6 Any information held within emails may be subject to release under a subject access request under the Data Protection Act 2018/UK General Data Protection Regulation (UK GDPR) or the Freedom of Information Act 2000 (FOIA). This will follow the Trusts standard process for requests including applying any redactions or exemptions where applicable.

2. SCOPE OF PROCEDURE

2.1 This procedure applies to anyone who has a Trust or School's within the Trust log-in ID and anyone who has been provided with access to the Trusts or School's within the Trusts internet or communications facilities.

2.2 The arrangements of this procedure may include checking the contents of and in some instances recording, email messages for the purpose of:

- Establishing the existence of facts relevant to the business.
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of email facilities.
- Ensuring effective operation of email facilities.
- Determining if communications are relevant to the business, e.g. where an employee is absent or on leave.

3. THE PROCEDURE

3.1 In circumstances where it is assessed that there has been a breach of the standards of acceptable use, as described in the Acceptable Use Policy, the Trust will as a first action, act promptly to prevent continuance or repetition of the breach. This action will be taken in accordance with the normal managerial arrangements and will typically involve liaison between the appropriate senior members(s) of the management team and the Trust's ICT partners.

3.2 Indications of non-compliance with the provisions of the Acceptable Use Policy will be investigated in accordance with the provisions of the Trust's Disciplinary Procedure.

3.3 Where access to an individual's internet or communications account/log is required for either the purposes of an investigation or any other reason mentioned in 2.2, an Access Form (Investigations) or Access Form (Absence) must be completed (see appendix 1 & 2) in order to assess the impact and decide if and how to carry out monitoring.

3.4 The Access Forms are provided in order to undertake an impact assessment which involves:

- Identifying clearly the rationale for the monitoring arrangements and the outcomes it is likely to deliver.
- Identifying any likely adverse impact of the monitoring arrangement.
- Considering alternatives to monitoring or different ways in which it might be carried out.
- Taking into account the obligations that arise from monitoring.
- Judging whether monitoring is justified in the circumstances.

3.5 All Access Forms must be forwarded to ICT, email address admin@thebeamtrust.co.uk in order that they can judge whether a monitoring arrangement is a proportionate response to the issue it seeks to address. This email address is a secure email that only a limited number of senior I.T. personnel have access to.

4. PROCEDURE FOR ACCESS TO EX-EMPLOYEE EMAIL ACCOUNTS

4.1 In some circumstances it will be necessary to access the email account of a former employee, e.g. to gain access to work related information that the user has stored on their email account and not copied to their headteacher/team/colleagues prior to leaving.

4.2 Headteachers/Managers should ask employees to clear their email accounts of personal emails so that only business emails remain on the account before they leave. If an individual is aware that business information they hold on their account will be required by the Trust or Schools within the Trusts at some future date it should be stored on disc.

5. PROCEDURE FOR ACCESS TO ABSENT EMPLOYEE EMAIL ACCOUNTS

5.1 If a member of staff is absent from work for any reason (e.g. sickness leave, annual leave, maternity leave etc) their permission should be sought to access their email account or personal folder. The employee should be made aware of what information needs to be accessed and only those emails/files should be opened. Anything marked personal or has a personal file name attached to it must not be opened.

5.2 Where permission cannot be obtained the headteacher/manager will need to contact the Trust's ICT partners and where appropriate, make arrangements for an appropriate member of the ICT team accompanied by a headteacher/manager to access the email account and open the relevant file.

6. ADVERSE IMPACT AND ALTERNATIVES

6.1 Identifying any likely adverse impact means taking into account the consequences of monitoring, not only for employees, but also for others who may be affected by it, such as customers.

6.2 When considering the impact, the following should be considered:

- What intrusion, if any, will there be into the private lives of employees and others, or interference with their private e-mails, telephone calls or other correspondence? Bear in mind that the private lives of workers can, and usually will, extend into the workplace.
- To what extent will workers and others know when either they, or information about them, are being monitored and then be in a position to act to limit any intrusion or other adverse impact on themselves?
- Whether information that is confidential, private or otherwise sensitive will be seen by those who do not have a business need to know, e.g. I.T. workers involved in the monitoring.
- What impact, if any, will there be on the relationship of mutual trust and confidence that should exist between workers and their employer?
- What impact, if any, will there be on other legitimate relationships, e.g. between trade union members and their representatives or between the worker and clients?
- What impact, if any, will there be on individuals with professional obligations of confidentiality or secrecy, e.g. solicitors or doctors?
- Whether the monitoring will be oppressive or demeaning.

6.3 Considering alternatives, or different methods of monitoring, means considering questions such as:

- Can established or new methods of supervision, effective training and/or clear communication from headteachers/managers, rather than electronic or other system monitoring, deliver acceptable results?
- Can the investigation of specific incidents or problems be relied on, for

example accessing stored emails to follow up an allegation of malpractice, rather than undertaking continuous monitoring?

- Can monitoring be limited to workers about whom complaints have been received, or about whom there are other grounds to suspect wrong-doing?
- Can monitoring be automated? If so will it be less intrusive, e.g. does it mean that private information will be 'seen' only by a machine rather than by other workers?

7. THIRD PARTY REQUESTS

7.1 The Trust and School's within the Trust's privacy notice states how the organisation handles and processes data in accordance with the Data Protection Act 2018 and/or UK GDPR. The Trust may have additional privacy notices for specific data use and projects, where these are not in place the corporate privacy notice is the one we refer to.

7.2 All third party requests will be reviewed on a case by case basis to ensure they are handled and processed in line with the Data Protection Act 2018 and/or UK GDPR and the associated lawful basis for processing which may be public task, legislation or consent.

7.3 The Trust reserves the right to ask third parties to submit formal requests for information for example via court order, solicitors letter or a police schedule 2 disclosure request form. Each request will be reviewed and risk assessed prior to any release of information.

8. LEGAL CONSEQUENCES OF MISUSE OF EMAIL FACILITIES

8.1 In a growing number of cases in civil or criminal law, email messages (delated or otherwise) are produced as evidence in a permanent written form. There are a number of areas of law which apply to the use of email and which could involve liability of users or the Trust.

These include the following:

- Intellectual property: Anyone who uses email to send or receive any materials that infringe the intellectual property rights of a third party may be liable to that third party if such use is not authorised by them.
- Obscenity: a criminal offence is committed if a person publishes any material which is pornographic, excessively violent or which comes under the provisions of the Obscene Publications Act 1959. Similarly the Protection of Children Act 1978 makes it an offence to publish or distribute obscene material of a child.
- Defamation: as a form of publication, the internet is within the scope of legislation relating to libel where a statement or opinion is published which adversely affects the reputation of a person, group of people or an organisation. Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or organization will rest mainly with the sender of the email and may lead to

substantial financial penalties being imposed.

- Data Protection: processing information (including photographs) which contains personal data about individuals, should only be undertaken where there is an established lawful basis under the Data Protection Act 2018 and/or UK General Data Protection Regulation (UK GDPR) such as legislation or public task.
- Discrimination: any material disseminated which is discriminatory or encourages discrimination may be unlawful under the Equality Act.

8.2 The above is only designed to be a brief outline of some of the legal consequences of misuse of email facilities.

9. FURTHER INFORMATION

9.1 Further advice and guidance on this procedure or the specific circumstances of a disciplinary matter can be obtained from the Trust's HR Business Partner.

9.2 If you would like to comment on the content of the procedure, please contact the Trust's HR Business Partners.

9.3 This procedure is also available in alternative formats or community languages if requested.

9.4 This policy links to the following sources of information.

- Acceptable Use Policy

ACCESS FORM (INVESTIGATIONS)

Information recorded on this form and any reports, recommendations and correspondence arising from this information will be processed by The Beam Trust in accordance with the Data Protection Act 1998 and all relevant legislation.

The Requesting Manager should complete all of Part 1 of the form (1A to 1D) and then forward it as an email attachment to the Authorising Manager (Assistant Director).

PART 1A – the Subject	
Name of Subject	
Job title of Subject	
Subject's team and directorate (or employer/organisation[1])	
Name of Subject's line manager	

PART 1B – details of the evidence being requested		
Please indicate which types of evidence you require. For each type that you need, please give the requested details.		
Available types of evidence	Do you need this? (YES or NO)	If you need this evidence, please answer the additional questions (below).
Internet activity		Questions 1B.1 to 1B.2
email account		Questions 1B.3 to 1B.5
Personal network drive		Questions 1B.6 to 1B.7
Physical computer hard drive		Question 1B.8
Other media (such as a portable memory device)		Question 1B.9
Additional questions (answer only those which apply)		
1B.1	What date is the Internet log to start?	
1B.2	What date is the Internet log to end?	
1B.3	Describe the monitoring you require on the above subjects email account. E.g. what are you looking for?	
1B.4	Do you also wish to see archived emails?	
1B.5	What is the timeline for this monitoring? E.g. if you are aware that what you are looking for is in a specific timeline, please state what that is to prevent excessive monitoring and workloads	
1B.6	Which personal network drive do you want to see?	
1B.7	What is the network drive path?	

[1] If the Subject does not work for The Beam Trust, then seek legal services advice before using the Access Procedure about the use of this procedure. Attach the advice to the Access Form.

1B.8	What is the asset tag on the computer?	
1B.9	Please specify what else you need access to, and where the item(s) is/are located.	

PART 1C – the impact assessment made by the Requesting Manager
1C.1 On what objective reason do you base your request for Access?
1C.2 Do you suspect that a specific provision in the Trust's Email, Internet or other Policy or Standard or Code of Practice has been contravened? Or what specific unlawful activity is suspected?
1C.3 Indicate the degree or seriousness of wrong doing suspected if any.
1C.4 Indicate the extent to which you expect to be looking at private emails or other private information.
1C.5 Consider intrusion into private information resulting from your access. What would be the possible adverse impact on the Subject, resulting from the disclosure of their private information.
1C.6 What are the alternative methods to obtain the information required, without looking at the evidence that is being requested, and why have they been discounted?
1C.7 Have HR and Internal Audit been consulted about this request / investigation? If so, please name the HR / Audit officer involved. If not, please give the reason why HR / Audit have not been consulted.
1C.8 Do you want to cross-reference this to any other request / investigations? If so, please give details.

PART 1D – details of the Requesting Manager	
Name	
Job title	
Team and Directorate (or organisation)	
Telephone number	
e-mail address	
Network login ID	

Guidance for the Requesting Manager – what to do next

- Save this form to your personal network drive, but make sure that no individual is identified within the document name.
- Attach the form to an e-mail and send it to the Authorising Manager. Begin the e-mail subject line with the word RESTRICTED and do not identify any individual within the subject line.

The Authorising Manager should complete all of Part 2 of the form (2A and 2B) and then forward it as an email attachment to the the following email address admin@thebeamtrust.co.uk

The email must be sent personally by the Authorising Manager and not by an assistant or by someone with delegated access to the manager's mailbox.

PART 2A – details of the Authorising Manager	
Name	
Job title	
Team and Directorate (or organisation)	
Telephone number	

PART 2B – Authorising Manager's consideration of the form	
Please answer YES or NO to each of the questions in this part.	
Are you aware that the Requesting Manager named in Part 1D is investigating the activity of the person named in Part 1A above?	
Are you satisfied that this access request is necessary and appropriate?	
Are you satisfied that this is an internal investigation into suspected wrongdoing and that an alternative route (such as RIPA) is not appropriate?	
Do you authorise the production of the investigation evidence and the provision of the evidence to the Requesting Manager?	

Guidance for Authorising Manager – what to do next

- If you wish to save a copy of this form, save it to your personal network drive, but make sure that no individual is identified within the document name.
- Attach the completed form to an e-mail and send it to the above email address. Begin the email subject line with the word RESTRICTED and do not identify any individual within the subject line.
- As Authorising Manager you are personally responsible for submitting the form; other staff may not submit it on your behalf.

Part 3 of the form is to be completed by a senior member of ICT

PART 3B – verification of form		
	Initials	**Date**
Check that all Parts have been fully completed.		
Check that the impact assessment (Part 1C) is adequate.		
Verify that the Requestor and the Authorising Manager are not the same person.		
Check the seniority of the Authorising Manager.		
Check that the answers in Part 2B are all 'yes', or establish why if not.		
Check that the completed form has been submitted from the Authorising Manager's personal mailbox and has not been sent by someone with delegated access.		