Seckford Foundation
a foundation for life

Data Protection Policy

Version Number:	V 2.0
Applies to:	Whole Foundation
Author (s):	Operations Bursar
Review Frequency:	2 yearly
Policy category (1, 2, 3, 4):	1
Last reviewed:	Michaelmas 2023
Next review due by:	Michaelmas 2025
Approved on (date):	C & R – 10.10.23 Governors – 23.11.23
Committee (s) Responsible:	Compliance and Risk (C & R) / Governors
References (including legal and others e.g., ISBA):	ISBA model policy
ISI Reg (if policy includes cover for WBS and an ISI reg is applicable):	NA
Other related policies and documents:	Online Safety Portfolio Data Retention Guidelines

Contents

1. Introduction

Data protection is an important legal compliance issue for The Seckford Foundation. During the course of the Foundation's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, volunteers, grant recipients and other individuals who come into contact with the Foundation. The Foundation, as "data controller", is liable for the actions of its staff and governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the UK GDPR) and the Data Protection Act 2018 (DPA 2018).

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law and will typically look into individuals' complaints routinely and without cost and has various powers to take action for breaches of the law.

2. Policy statement

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the Foundation's culture, and all its staff and representatives need to be mindful of it

3. Definitions

Key data protection terms used in this data protection policy are:

- Data controller – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the Foundation (including by its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.
- Data processor – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
- Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- Personal information (or 'personal data'): any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the Foundation's, or any person's, intentions towards that individual.
- Processing – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
- Special categories of personal data – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

4. Policy

This policy sets out the Foundation's expectations and procedures with respect to processing any personal data we collect from data subjects (including, employees, contractors and third parties).

Those who handle personal data as employees or governors of the Foundation are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the Foundation or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the Foundation's personal data as contractors, whether they are acting as "data processors" on the Foundation's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

Where the Foundation shares personal data with third party data controllers – which may range from other charitable organisations, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

5. The Principles

The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed lawfully, fairly and in a transparent manner.
2. Collected for specific and explicit purposes and only for the purposes it was collected for.
3. Relevant and limited to what is necessary for the purposes it is processed.
4. Accurate and kept up to date.
5. Kept for no longer than is necessary for the purposes for which it is processed.
6. Processed in a manner that ensures appropriate security of the personal data.

The UK GDPR's broader 'accountability' principle also requires that the Foundation not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

- Keeping records of our data processing activities, including by way of logs and policies.
- Documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments).
- Generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected

from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

6. Lawful grounds for data processing

Under the UK GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under UK GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the Foundation to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the Foundation. It can be challenged by data subjects and also means the Foundation is taking on extra responsibility for considering and protecting people's rights and interests. The Foundation's legitimate interests are set out in its Privacy Notice, as UK GDPR requires.

Other lawful grounds include:

- Compliance with a legal obligation, including in connection with employment, engagement of services and diversity.
- Contractual necessity, e.g., to perform a contract with staff, or the engagement of contractors.
- A narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

7. Roles and Responsibilities

The Foundation has appointed Richard Stone (Operations Bursar) as the Data Protection Officer (DPO) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of applicable data protection legislation. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

7.1. Record Keeping

It is important that personal data held by the Foundation is accurate, fair and adequate. Staff are required to inform the Foundation if they believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on Foundation business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues, in accordance with the Foundation's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for

staff is to **record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.**

7.2. Data Handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with all relevant Foundation policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the Foundation's wider responsibilities such as IT security. Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

7.3. Avoiding, mitigating and reporting data breaches

One of the key obligations contained in the UK GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the Foundation must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach they must notify the DPO. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the Foundation always needs to know about them to make a decision.

As stated above, the Foundation may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the Foundation, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

7.4. Care and data security

More generally, we require all Foundation staff (and expect all our contractors) to remain mindful of the data protection principles, and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the Foundation to the DPO, and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to

7.5. Use of third party platforms / suppliers

As noted above, where a third party is processing personal data on the Foundation's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to the DPO in the first instance, and at as early a stage as possible.

8. Rights of Individuals

In addition to the Foundation's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the Foundation). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the DPO as soon as possible.

Individuals also have legal rights to:

- Require us to correct the personal data we hold about them if it is inaccurate.
- Request that we erase their personal data (in certain circumstances).
- Request that we restrict our data processing activities (in certain circumstances).
- Receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller
- Object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- Object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention).
- Object to direct marketing.
- Withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the DPO as soon as possible.

9. Data security: online and digital

The Foundation must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

As a member of the Foundation you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the Foundation (for example, content that is obscene, or promotes violence, discrimination, or extremism).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the Foundation, even if the content is shared publicly.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils, parents or care residents and their families, and pupils, parents, care residents and their families should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Whenever you use the Foundation's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access Foundation IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the Foundation's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, Foundation IT systems.
- Do not use the Foundation's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the Foundation monitors use of the Foundation's IT systems, and that the Foundation can view content accessed or sent via its systems.

10. Processing of Financial / Credit Card Data

The Foundation complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard, please seek further guidance from the Finance Director. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

11. Seckford Foundation Archive

The Seckford Foundation archive is maintained as a resource to help inspire and equip current staff, pupils and residents to understand and appreciate issues of identity, belonging and shared heritage; to prompt memories among many generations of staff, pupils and residents; and to serve as a research resource for all interested in the history of The Seckford Foundation and the community it serves.

12. Compliance and Monitoring arrangements

This policy will be subject to a thorough review process including consideration at the Compliance and Risk Committee and ratification by the Governing Body every 2 years. This will ensure that practice across the whole foundation is in line with this policy, the Complaints procedure and with current guidance and legislation.