Plan International UK

Data and Cyber Accountability Statement

('How we do data protection and cyber security at Plan International UK')

DOCUMENT CONTROL INFORMATION:

Title	Data and Cyber Accountability Statement
Author (Responsible)	Head of IT (Data Protection Officer)
Owner (Accountable)	Director of Finance and IT
Directorate	Finance and IT
Contact	Head of IT
Version	2.0
Status	Approved
Reviewed by (Consulted)	Data and Cyber Group
Approved by	Leadership Team
Date of Approval	May 2023
Applicable to (Informed)	All IT System Users (statement published on website)
Issued on	2nd June 2023
Date of next review	May 2026
Related policies & procedures	Data Protection Policy, Data Retention Policy, Information Security Policy, IT User Policy, Procurement Policy, Contract Signing Policy

DECISION-MAKING:

Decision	Accountable	Responsible	Consulted	Informed
All matters concerning this statement	Director of Finance and IT	Head of IT	Data and Cyber Group	All staff, all stakeholders (via website)

Introduction to Data Protection and Cyber Security Accountability at Plan International UK

As part of Plan UK's compliance with the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications Regulations (PECR), guidance issued by the ICO, and guidance published by the National Centre for Cyber Security ("NCCS") Plan UK has reviewed how we demonstrate accountability for our data processing and cyber security activities as part of our ongoing compliance activities.

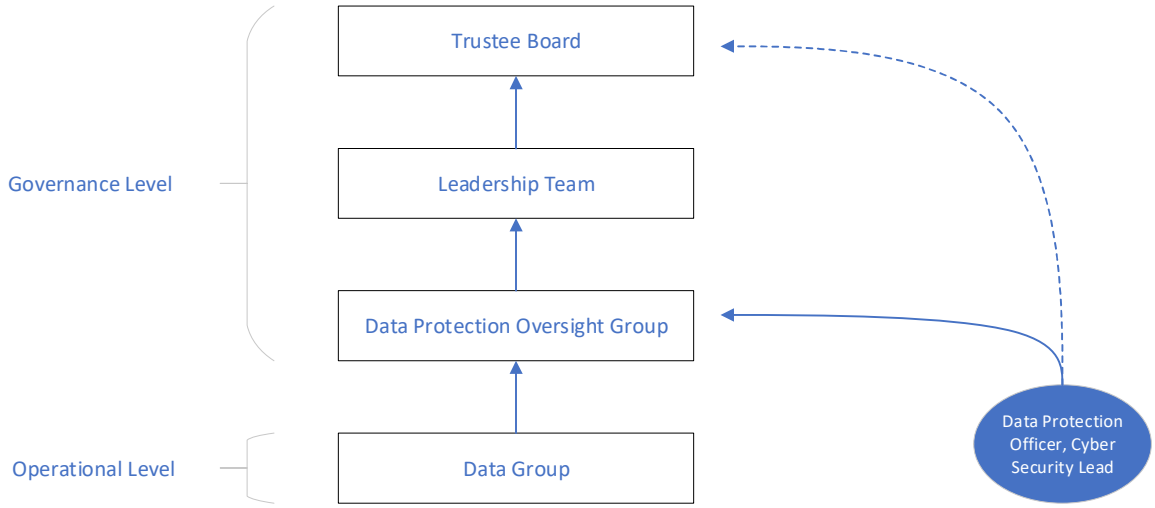
Plan UK recognises that Data Protection and Cyber Security are distinct disciplines, but also that there is considerable overlap between the two. Activities carried out to improve Cyber Security also tend to benefit Data Protection and vice-versa. As a result, at Plan UK, Data Protection and Cyber Security are subject to similar governance arrangements. This document explains how this arrangement is constructed, governed, managed, and resourced.

Governance Summary

Plan UK runs quarterly 'Data and Cyber Group' meetings - chaired by the Chief Executive, with senior level attendance - in order to ensure an effective data protection compliance framework is in place and to ensure data protection/cyber security risks and issues are dealt with at an appropriately senior level. See Appendix D for the Terms of Reference.

Plan also administers quarterly 'Data Group' meetings, chaired by the Data Protection Officer ("DPO"), which are attended by Data Protection and Cyber Security Allies from across the business to discuss information / cyber compliance work and to improve awareness across the organisation. See Appendix E for the TOR.

This overall governance and reporting structure is summarised in the diagram below:



Key Roles

Plan UK is not a public authority and does not carry out large scale processing of special category data or data relating to criminal convictions and offences. However, Plan UK's core activities do

involve large scale regular processing of personal data and Plan UK has therefore voluntarily appointed an independent DPO in compliance with Article 37 of UK GDPR. Plan UK has also created a Cyber Security Lead (CSL) role, both of which report into the Senior Information Risk Officer (SIRO).

Plan UK also recognises that effective Data Protection and Cyber Security measures require understanding and buy-in from across the organisation – the responsibility does not sit with the SIRO, DPO, and CSL alone. Therefore, Plan UK has appointed Information Asset Owners (IAOs). These are the directors within the Leadership Team of Plan UK, and they are accountable for the Cyber Security and Data Protection within their teams. The IAOs are also responsible for appointing Data Protection and Cyber Security Allies within their teams who are the front line of Data Protection and Cyber Security compliance and have a strong working knowledge of the day-to day activities within their teams.

Collectively, Plan UK has appointed a number of roles across the organisation to ensure an appropriate level of Data Protection and Cyber Security Compliance:

- The SIRO champions Information Security at the highest levels of management
- The DPO has the lead role in ensuring Plan UK's data protection accountability, in line with the legislative requirements for this role
- The CSL has overall responsibility for Cyber Security within Plan UK and ensures that regular Cyber Security related activities take place
- Information Asset Owners are senior managers with accountability for the teams they oversee
- Data Protection and Cyber Security Allies have a strong working knowledge of day-to-day activities and compliance within their teams.

These roles are defined in more detail in Appendices A-C.

Independence

Our DPO and CSL are able to raise issues in the way they see fit, without approval from their director (the SIRO) or others to do so. The DPO/CSL also have a dotted line reporting mechanism into a lead Data Protection trustee, and thus the Trustee Board. Our DPO/CSL is not penalised for performing their tasks or challenging the business in matters relating to data protection/cyber security.

Reporting to highest level of management

The DPO and CSL are accountable to Plan UK's Leadership Team, the most senior management body at Plan UK, (which therefore includes the SIRO).

The DPO and CSL provide an annual summary report to Leadership Team and the Trustee Board as well as reporting more frequently, including immediately, should the need arise (e.g. in the case of a data breach that was reportable to the Information Commissioner's Office).

The DPO and CSL are responsible for reporting risks or opportunities and recommending appropriate actions in relation to Plan UK's cyber security or processing of personal information.

Both roles have access to all of our information systems and access to all services and staff if they need input, information or support.

DPO tasks

The requirements of Article 39, as described by the ICO, are included in the DPO role profile, and have been formally approved by Leadership Team. Plan UK has appointed an internal employee as our DPO who has additional professional duties. As DPO and Head of IT, the tasks and focus of each role are reasonably complementary – and sitting in IT provides additional intelligence in terms of knowing about new systems or processes in development. The DPO and CSL are encouraged to raise any conflict-of-interest concerns with the Trustee Board.

Visibility

Our DPO's contact details are included within our privacy information and records of processing activities. We also include their contact details as part of the IT induction, which is completed by all staff. We have a dedicated email address and monitored inbox for data protection queries or complaints received internally or externally. Our DPO is our contact with the Information Commissioner's Office in its capacity as UK supervisory authority.

Decision making

Where the advice of the DPO or CSL is not followed, this is documented.

Organisational and Technical measures:

Plan UK recognises that strong Cyber Security and Data Protection practice requires the application of both technical and organisational measures.

(a) Organisational

Plan UK maintains a suite of policies and procedures, including the Information Security and Data Protection Policies which enables Plan to embed cultural and systematic good practice, identify and manage our cyber/information risks, and monitor compliance.

Alongside these key policies, Plan UK also maintains key accountability documentation including a record of processing activities (ROPA), and a Data Retention Policy. The data protection policy ensures that data subjects whose personal data we process will be made aware of the privacy notice which is published on Plan UK's website. In addition to data and cyber risks being on the organisational risk register, Plan UK also maintains data protection and cyber security risk registers that are reviewed quarterly by the Data and Cyber Group.

The approach has 'privacy by design and default' at the forefront. We have an established Data Protection Impact Assessment process to ensure information and cyber risks are thought about during the early stages of all work. This process is linked to and signposted from the procurement, supplier assessment and contract management processes, and training is provided to all Data Protection and Cyber Security Allies, and available to staff/teams on request.

Online training in both Data Protection and Cyber Security is mandatory for all staff/volunteers/trustees and must be completed annually.

(b) Technical

Plan UK follows the NCCS guidance in the following ways :

- All data is securely backed up to a cloud-based location
- All Plan UK issued Smartphones have passwords and encryption applied, as detailed in our Mobile Device Policy
- We use Anti-virus software on all devices and have an agreed monthly system maintenance window during which any security patches can be applied
- We mandate cybercrime training for all staff/volunteers/trustees and run regular phishing tests
- We maintain a Password Policy so that the passwords used by Plan UK are as effective as possible in preventing unauthorised access to Plan's devices and data
- We maintain an Internet Content Filtering Policy so that Plan UK can scan/monitor internet traffic proportionately to the risk posed

Plan UK's Data Protection and Cyber Security compliance is also regularly externally assessed, recent examples include :

- A GDPR audit in 2018
- An IT Controls audit in 2020
- An ISO 27001 based Cyber Security review in 2021
- An internal controls audit in 2023
- Annual Penetration Testing
- Annual maintenance of Cyber Essentials Plus accreditation
- Annual maintenance of PCI-DSS accreditation
- Six-monthly penetration testing

Finally, Plan UK combines measures of training completion rates, results from phishing tests, scores from penetration tests and the Microsoft Secure score into an organisation-wide 'Security KPI' which is published quarterly.

APPENDIX A: Data Protection Officer (DPO) Role

ICO Guidelines

The DPO role, according to the Information Commissioner's Office (ICO), must:

- Report to the highest level of management
- Be sufficiently well resourced to perform their tasks
- Be able to operate independently, and not be penalised for performing DPO duties
- Be involved in a timely manner in all issues relating to the protection of personal data
- Not undertake other tasks or duties which result in a conflict of interests with their DPO duties

Plan UK Implementation

At Plan UK, our DPO is the Head of IT and is responsible for:

- Informing and advising the organisation, its employees and trustees about their obligations under GDPR. This includes a 'dotted line' report into the Trustee Board
- Monitoring compliance with GDPR and related legislation and providing Leadership Team and Trustee Board with an annual summary report, as well as more frequent reporting, as required
- Being the external point of contact for data enquiries as per the general Privacy Notice on Plan UK's website and for any supervisory authorities, e.g. the ICO
- Overseeing the maintenance of Plan UK's data processing activities (ROPA)
- Leading on decisions relating to the requirement of Data Protection Impact Assessments (DPIAs) and their subsequent review
- Leading on the processing of Subject Access Requests
- Leading on the reporting and processing of any data breaches, including advising on action to prevent, or reduce likelihood of, recurrence
- Ensuring that effective data protection training for staff is in place
- Attending and reporting as required to the Data Protection Oversight Group
- Organising and chairing the Data Group meetings
- Presenting work proposals to the Data Protection Oversight Group and Data Group which ensure that the highest risk areas of data processing are regularly examined and any remedial actions carried out.

APPENDIX B: Cyber Security Lead (CSL) Role

General Considerations

A CSL is a senior manager with an with overall responsibility for the organisation's approach to managing cyber related risk. It is not a legally mandated or defined role, but is generally considered to have the following responsibilities:

- To provide board level accountability and assurance that cyber risks are being appropriately managed and addressed
- To ensure the maintenance of an appropriate Cyber risk register
- To be a champion for developing a culture which values Cyber Security and is visible in doing so across the organisation
- To regularly report to the most senior level of management, and ensure that Cyber Security awareness remains high and is understood to be a responsibility which is shared across the entire organisation.

Plan UK Implementation

At Plan UK, our CSL is the Senior IT Operations and Infrastructure Manager and is responsible for:

- Providing Leadership Team and Trustee Board with a senior point of contact responsible for Cyber Risk
- Ensuring the cyber risk register is reviewed quarterly and risks communicated to the Data and Cyber Group (or Leadership Team) as appropriate
- Providing challenge to Leadership Team, or the business, as appropriate, if it is felt that cyber compliance is not being given the importance it requires
- Fostering a culture of high cyber security awareness, including providing training to staff as agreed within the Information Security Policy
- Developing a learning culture to allow Plan UK to understand where cyber issues may arise and develop appropriate solutions to prevent problems occurring

APPENDIX C: Senior Information Risk Officer (SIRO) Role

General Considerations

A SIRO is the member on the Management Board of an organisation with overall responsibility for the organisation's approach to managing information and cyber risk. It is not a legally mandated or defined role, but is generally considered to have the following responsibilities:

- To provide senior management level accountability and assurance that information/cyber risks are being appropriately managed and addressed
- To ensure the maintenance of an appropriate Information Governance and Cyber Security Framework
- To be a champion for developing a culture which values Information Governance and Cyber Security and supports the principle of data protection by design and default
- To be an executive-level champion for the concept of information and cyber security as an asset/enabler. Information and Cyber is integral to the functioning of modern business and essential to delivering corporate objectives.
- To be the ultimate decision maker in deciding when to report any data protection or cyber security breach (for example to the ICO or Charity Commission)

Plan UK Implementation

At Plan UK, our SIRO is the Interim Director of Finance and Resource and is responsible for:

- Providing Leadership Team and Trustee Board with a senior point of contact responsible for Information/Cyber Risk
- Ensuring the data protection and cyber security risk registers are reviewed quarterly and risks communicated to Leadership Team as appropriate
- Line management of the DPO role, and ensuring the DPO's efforts are concentrated in the areas of most business value to Plan UK
- Providing challenge to Leadership Team, or the business, as appropriate, if it is felt that data protection/cyber compliance is not being given the importance it requires
- Providing challenge to the DPO, as appropriate, if it is felt that non-legislatively required compliance work is not proportionate to business needs
- Fostering a culture of cyber security awareness and data protection by design and default, including providing high level support to the DPO where appropriate/required
- Developing a learning culture to allow Plan UK to understand where data protection / cyber issues may arise and develop appropriate solutions to prevent problems occurring

APPENDIX D: Terms of Reference – Data and Cyber Group

Introduction

One of the key principles of the GDPR legislation is for data controllers (i.e. Plan International UK, PIUK) to be able to demonstrate their compliance. It is expected that appropriate technical and organisational measures are in place to safeguard any personal data that is processed. The ICO also expects the accountability methods and measures to be reviewed at appropriate intervals, with suitable senior management oversight. Furthermore, the NCCS points out that 'Charities are not immune to cyber crime' and that 'everybody involved with charities… has a role to play in protecting the charity sector from cyber-related harm'.

Purpose

The purpose of the Data and Cyber Group is to:

- Reviewcompliance with the overall framework of data protection legislative measures, for example (but not limited to) GDPR, The Data Protection Act 2018, PECR
- Receive reports on compliance with Cyber related measures such as Cyber Essentials Plus, PCI-DSS, annual penetration testing, phishing tests, and cyber-related training completion rates
- Oversee the organisation's cyber / data protection responsibilities in key business areas to ensure compliance, and ownership of the resulting levels of risk, including maintaining data protection and cyber security risk registers
- Ensure an effective cyber / data protection compliance framework is in place and maintained and to own the organisational approach to compliance including all policies and procedures within this framework
- Review summary information about Cyber Incidents, Data Protection breaches, and Subject Access Requests, providing input, challenge and decision making where required
- Review annual summary report to Leadership Team and Trustee Board, as well as more frequent reporting, as required

The Data Protection Oversight Group will review these terms of reference periodically, with any proposed changes to be approved by Leadership Team.

Membership

- Chief Executive (Chair)
- Senior Information Risk Officer (SIRO, also Chief Operating Officer)
- Data Protection Officer (DPO, also Head of IT)
- Data Protection Consultant
- Cyber Security Lead (CSL, Senior IT Infrastructure and Operations Manager)
- Legal Counsel
- Other staff members may attend as requested by the Chair

Meetings

The Data Protection Oversight Group meets quarterly, typically for 2 hours. The DPO organises the meetings and takes and circulates minutes and actions from each meeting. The minutes record decisions made, items formally noted and action to be taken. Additional discussions/decisions may take place by email as required.

A draft agenda will be produced two weeks before the meeting by the DPO and circulated to all members, with a final agenda and papers sent one week before each meeting, so that all papers can be read ahead of the meeting.

APPENDIX E: Terms of Reference – Data Group

Introduction

One of the key principles of the GDPR legislation is for data controllers (i.e. Plan International UK, PIUK) to be able to demonstrate their compliance. It is expected that appropriate technical and organisational measures are put in place to safeguard any personal data that is processed, with suitable involvement of applicable staff. Furthermore, the NCSC points out that 'Charities are not immune to cyber crime' and that 'everybody involved with charities… has a role to play in protecting the charity sector from cyber-related harm'.

Purpose

The purpose of the Data Group is to:

- Consider and agree the appropriate prioritisation of ongoing compliance work, e.g. updating the Register of Processing Activities (ROPA) and selection of Vulnerability Assessment initiatives
- To determine whether there are any areas where PIUK's cyber security or processing of data might be improved, or where Data Protection Impact Assessments may be required, supporting the Information Asset Owners to ensure that that their units are compliant with cyber and data related legislation
- Disseminate information and learning from the Data Group meetings back to the teams within the organisation with a view to building and improving an organisational culture of cyber security and data protection awareness
- Advise and support the Data and Cyber Group on data compliance issues, providing specialist knowledge, and feeding into the Data Protection and Cyber Security risk registers

The Data and Cyber Group will review these terms of reference at least every 3 years, with any proposed changes notified to Leadership Team.

Membership

In line with its purpose above, the Data Group is made up of Data Protection and Cyber Security Allies who have been appointed by IAOs from all directorates. If staff are unable to attend, they should send an appropriate deputy in their place. Attendees must be able to communicate information to and from their directorate with respect to all Data Group matters.

Meetings

The Data Group meets quarterly for 2 hours. The DPO (or otherwise as appointed by the DPO, as Chair) organises the meetings and takes and circulates minutes and actions from each meeting. The minutes record decisions made, items formally noted and action to be taken. Additional discussions/decisions may take place by email as required.

A draft agenda will be produced two weeks before the meeting by the DPO and circulated to all members, with a final agenda and papers sent one at least two working days before each meeting, so that all papers can be read ahead of the meeting. Attendees are expected to bring their own hard copies of papers.

APPENDIX F: Alignment with Global Policy on Data Privacy

In 2022 Plan International agreed the Global Policy on Data Privacy. As part of its scope, National Organisations are expected to 'enact their own procedures, regulations, or other regulatory documents that support compliance…with this Global Policy'. Plan UK believes that it is aligned with the Global policy based on the assessment against the 11 global principles below, approved by the Data Protection Oversight Group in April 2023

Global Principle	How Plan UK meets this principle
1. Contact Details	Plan UK ensures the availability of Data Controller's identity and DPO's contact details whenever personal data is collected from a subject (privacy statement published on Plan UK's website)
2. Fairness, Legitimacy, and Transparency	Plan UK records the lawful basis for processing within the ROPA and all Data protection impact assessments. Plan UK provides a privacy notice (or access to one) every time personal data is collected
3. Personal data of children	As a National Organisation Plan UK processes a relatively small amount of personal data relating to children (principle of minimisation) .Plan UK has sought specialist advice in ensuring privacy notices are written in easily accessible and plain language
4. Purpose Specification and limits on secondary use	Legitimate interest tests are carried out whenever a legitimate interest argument is made for the use of personal data
5. Information provided to data subjects	Information about the purpose, lawful basis, subject's rights, retention, third party disclosure are provided in the privacy notices
6. Data minimisation and accuracy	Data minimisation is queried during any Data protection impact assessment process. Data inaccuracies, when identified are rectified without undue delay
7. Data retention and destruction	Plan UK has an agreed set of processes as formally recorded within the Plan UK Retention Policy
8. Confidentiality and Security	Plan UK has an Information Security Policy and uses UK/EU based hosting environments, all of which are ISO 27001 certified
9. Personal Data Security Incidents	Plan UK maintains a Personal Data / Cyber Incident Breach process and maintains a central log of all breaches
10. Personal Data Transfers	How and when transfers occur is detailed within the privacy notices. International Transfer guidance within the Data Protection Policy
11. Training and Monitoring	Data protection and cyber crime awareness training is mandatory for all staff, volunteers and trustees. It is to be completed annually and training completion rates are reported/reviewed on a quarterly basis by the Data and Cyber Group