PEACEPLUS
Northern Ireland - Ireland
Co-funded by the
European Union | UK Government

Peace
Northern Ireland - Ireland
European Regional Development Fund

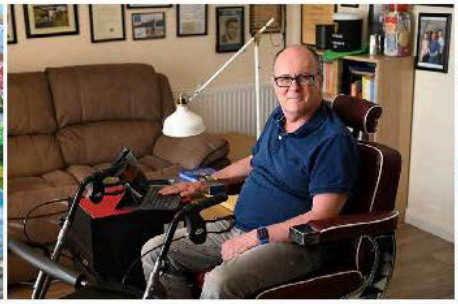
Interreg
Northern Ireland - Ireland - Scotland
European Regional Development Fund

Special EU Programmes Body
Comhlacht na gClár Speisialta AE
Special EU Skemes Boadie

SPECIAL EU PROGRAMMES BODY

# CANDIDATE BOOKLET

## IT Security Officer
## Belfast
## (3 Year Fixed Term Contract)


Northern Ireland Executive
www.northernireland.gov.uk

Rialtas na hÉireann
Government of Ireland

# Contents

# FOREWORD

Thank you for your interest in a role with the Special EU Programmes Body (SEUPB).

Our approach is simple: We seek the best people, hire them, and provide them with the tools and support they need to realise their full potential. Our role is an extremely important one for society, and therefore we require experience, enthusiasm, and energy to help us contribute to improving the lives of our citizens.

This is an exciting opportunity for a highly skilled and experienced professional to join SEUPB at a pivotal moment in its history, as we implement a new wide ranging funding Programme, and convey the impact that funding has on the lives of the citizens in the region.

We are one of six cross-border bodies set up under the Belfast/Good Friday Agreement, we have the statutory remit for the management of the EU cross border co-operation programmes, and we are currently concluding on two of those Programmes, while mobilising the roll out of the new successor programme PEACEPLUS.

PEACEPLUS is a European Union funding programme supported and developed in partnership with the European Commission, the Governments of the United Kingdom and Ireland and the Northern Ireland Executive, with a value of €1.144 billion. We consider it a privilege, to have this funding package secured for the benefit of our citizens in Northern Ireland and the six border counties of Ireland, especially in this current economic environment.

We have a wide range of stakeholders as we are directly accountable to the North South Ministerial Council, and we report to the European Commission, the Government of Ireland, and the Northern Ireland Executive. We work closely with most of the government departments in both jurisdictions, and key statutory agencies alongside the community and voluntary sector, and the private sector.

SEUPB has three offices, located in Belfast, Omagh and Monaghan.

This booklet provides further information on the key responsibilities of the role you have applied for and sets out the skills and competencies required.

**Gina** McIntyre

**Chief Executive**

**Special EU Programmes Body**

# INTRODUCTION

The SEUPB is responsible for the PEACE IV and INTERREG VA Programmes and the current PEACEPLUS Programme for the 2021-2027 period and beyond. Our role is to help facilitate the positive impact that European Regional Development Funding will have on the lives of people living across Northern Ireland and the border counties of Ireland.

We are one of the six cross-border Bodies created under the "Agreement between the Government of Ireland and the Government of the United Kingdom of Great Britain and Northern Ireland establishing implementing bodies" signed on 8 March 1999 (the British-Irish Agreement of 8 March 1999).

The Agreement was given domestic effect, North and South, by means of the North/South Co-Operation (Implementation Bodies) (Northern Ireland) Order 1999 and the British-Irish Agreement Act 1999 respectively.
We are responsible to two Sponsor Departments, the Department of Finance (DoF) in Northern Ireland and the Department of Public Expenditure and Reform (DPER) in Ireland, along with the European Commission and the North South Ministerial Council.

**SEUPB Mission Statement:**
***"To improve people's lives through partnership and cross border cooperation."***

**SEUPB Vision Statement:**
***"We will contribute to the development of a peaceful and prosperous society; striving to continually improve, drive simplicity and inspire our staff to be the best that they can be."***

**Our Guiding Principles:**
***In carrying out our work we will adhere to the following guiding principles:***

- ***We will deliver our mission, striving for excellence at all times. We subscribe to the principle of accountability and are prepared to be held accountable for all that we do.***
- ***We will act at all times with the interests of our stakeholders, beneficiaries and the public to the fore and demonstrate the highest levels of integrity in ensuring the mission of the SEUPB is delivered.***
- ***We will demonstrate equality and respect in all that we do and with everyone that we meet and work with***.

# THE PLAN FOR 2023-2025

2023 will see SEUPB closing the PEACE IV and INTERREG VA programmes and opening the PEACEPLUS programme.

The PEACE IV Programme, with a value of approximately €270 million, has provided support to projects which focus on four key objectives: Shared Education; Children and Young People; Shared Spaces and Services; and Building Positive Relations.

With a value of €283 million, the INTERREG VA Programme focuses on research and innovation to support economic development and projects under the themes of Environmental Protection, Sustainable Transport and Health Services.

The new PEACEPLUS Programme, with continued commitment and funding from the European Union, the Governments of the United Kingdom and Ireland, and the EU, is be valued at €1.1 billion.

The objective of the PEACEPLUS Programme is to build peace and prosperity and leave a lasting and tangible legacy across Northern Ireland and the border counties of Ireland. The Programme will help to address many long-standing social and economic challenges which have, and continue to impact on communities, particularly those in rural border areas, as well as ongoing challenges that exist in urban settings.

PEACEPLUS has been divided into six funded themes:

1. Building Peaceful and Thriving Communities
2. Delivering Socio-Economic Regeneration and Transformation
3. Empowering and Investing in our Young People
4. Healthy and Inclusive Communities
5. Supporting a Sustainable and Better-Connected Future
6. Building and Embedding Partnership and Collaboration.

Each theme aims to address longstanding social, environmental, and economic challenges. Within each theme there are several investment areas – these will have a more specific focus and target organisations such as local authorities or community groups.

It is vital we continue to provide opportunities for our community to interact and get to know each other by playing together and talking to each other. They must also have the very real prospect of living in a sustainable, healthy environment - in peace and without the threat of violence.

We have adjusted and adapted to a new way of working during the Covid-19 crisis and we will continue to assist projects so they can continue delivering the very important work they do. While the impact of this crisis is being truly felt by all of us, we are committed to doing what we can to assist and we understand there will be difficult times ahead, both socially and economically.
As an organisation, The Special EU Programmes Body is constantly striving to improve service delivery in support of our customers.

# SUMMARY OF JOB:

To provide an effective cyber security support service to the IT team and the overall business. This role requires a suitably qualified and experienced cyber security resource to take the lead with routine IT Security tasks, such as monitoring IT Security Systems and portals. The role will be responsible for implementation of the SEUPBs Cyber Security Strategy, it will also provide continuous review and implementation of IT security policies and procedures, it will provide an audit and compliance function within the IT team to ensure best practice is followed at all times, it will also provide IT security accountability and implementation of certification requirements for Public Sector bodies.

## KEY ASPECTS OF THE POSITION:

- Monitor, Maintain and Administer existing IT Security Platforms
- SIEM, XDR, MDM, Cloud VPN, Antivirus, Microsoft 365
- Develop, Implement, and routinely review IT Security Policies
- Incident Management / Response Planning
- Threat Vulnerability Management (TVM) Process is followed.
- IT Security Support and advisory function to IT Team and SEUPB
- Work with Information Officers to provide an Information Security Function
- Supplier Assurance Framework compliance for the business
- Maintaining Data Loss Protection standards for the business
- Cyber & Information Security Training Support for SEUPB staff
- Build solid partnerships with external service providers e.g. CISO, DPO
- Develop reports for IT Manager and Senior Management Exec Team
- Keep abreast of new Cyber Security Threats

## KEY RESPONSIBILITIES:

- Monitor, Maintain and Administer existing SEUPB IT Security Platforms.
- Management of exiting security platforms and portals; Review and act upon security events or alerts logged on the following platforms.
- XDR  Enrolment, Incident logging/reporting, investigation, and remediation, keep up to speed with new versions/features, attend online Palo seminars/webinars/events.
- Provide security input to the IT team on areas for configuration, update, or review of our Secure Remote Access service.
- Provide security input to the IT team on areas which maybe improved in our configurations/management of email scanning.
- Antivirus General monitoring of portal to ensure issues are addressed in time, e.g. outdated definitions or other warnings.
- Microsoft 365 – Security functions – ensure SEUPB MS 365 platform is secure and remains secure based on NCSC cloud principles
- SIEM Portal – Work with existing SOC managed service to ensure any incidents reported are followed up and investigated/remediated on time.
- Work with the IT Team to ensure team is up to speed with evolving Cyber Threats.

- Work in partnership with the IT Team to manage implementation of Threat & Vulnerability Management (TVM) process, ensuring systems are tested and risks are considered, remediation where needed is carried out, and all actions logged.
- Investigate suspected and actual cyber security breaches and incidents in accordance with the SEUPB Cyber Security incident management plan, and ensure any remedial action and lessons learned is conducted.
- Provide IT Manager with Monthly reports/dashboards on IT Security Posture, e.g. Server/Workstation Patch status, Risks, Incidents and Policy.
- Develop, Implement, and routinely review IT Security Policies & Strategy
- Provide strategic input to SEUPB IT Strategy which incorporates forward thinking for Security best practice
- Ensure identified areas for Cyber Security within the strategy are implemented as described.
- Constantly review and provide recommendations for updating the existing SEUPB Cyber Security Policy (work with CISO)
- Advise and implement as necessary any new Policies and/or Procedures to further improve SEUPB Cyber Security posture.
- Develop, manage, and maintain a Cyber Security Risk register which incorporates technology and information security risks
- Put in place a programme to review all IT Policies on an annual basis with Security in mind, especially policies directly responsible for adherence to security, e.g. User Access Policy
- Manage programme for Security Testing of SEUPB IT estate, to include all security testing requirements identified from CSMA and any other areas as identified.
- Provide input to Business Continuity plans, Disaster Recovery plans and Incident response plans.
- Manage a Cyber Security Awareness Programme, to include training for staff and regular testing

### Incident Management / Response Planning

- Ensure Incident Response plan is kept updated and fit for purpose.  Manage incidents as they are reported on various portals identified above.
- Work with the IT Manager and IT Team to manage any incidents as they arise.
- Liaise with all associated external parties in the event of an incident occurring.

### Provide an Audit & Compliance Function

- Provide an internal security audit role on existing IT and Information Management functions.
- Ensure any considerations for new systems or solutions, or changes to existing solutions have security considerations in place.
- Manage a programme to ensure Cyber Essentials Plus achievement is maintained annually.
- Ensure SEUPB is aligned to various information security frameworks such as CAF, NIST and NIS.
- Develop, Implement and Coordinate a programme of Pen Testing and IT Health Checks of identified key systems both internally and externally hosted.
- Ensure Threat Vulnerability Management (TVM) Process is followed

This role will own the Vulnerability Management Policy and Process and ensure it is implemented as designed. Below is a short description of how the policy is structured and where the responsibilities of this role are aligned.

| Monitor | Assess | Mitigate | Verify |
|---|---|---|---|

**Monitor:** There are several ways that vulnerabilities in the SEUPB IT environment can be identified to provide a holistic picture of the potential risks to the IT environment which could present a business risk. The following are sources of vulnerability information: Vulnerability Scanning Tools, Patch Management Tools, Mobile Device Management Tools, IT Heath Checks/3rd Party Vulnerability Assessments Other Intelligence Feed.

**Assess:** Setup and manage a vulnerability triage team, consisting of staff with knowledge of cyber security risk, business risk and IT estate management. The vulnerability triage team will review the assigned Common Vulnerability Scoring System (CVSS) Severity Rating, along with industry knowledge of current threats to assess actual risk to SEUPB based on all the available information at the time and identify the applicability of the reported vulnerabilities to the SEUPB Service applicable vulnerabilities will be categorised into three categories Fix, Acknowledge, and Investigate.

**Mitigate:** Successfully roll out the approved remediations into the operational environment whilst minimising impact on business.

**Verify:** This phase ensures that compliance checking is carried out at defined intervals against assets to verify the effectiveness of the process. This is to include Vulnerability scanning of the environment as a validation process to ensure that deployment and patching procedures are functioning properly.

### IT Security Support and advisory function to IT Team and SEUPB

- Work in partnership with IT Team to ensure Cyber Security is always to the forefront of existing IT Systems & Projects, and any potential future projects.
- Work with all teams in SEUPB regarding Cyber Security and with a view to protecting any Information Asset under SEUPBs responsibility.
- Work with HR Team to ensure quarterly reviews are undertaken regarding existing staff and leavers and ensure IT Team are aware of changes so that IT user accounts can be appropriately managed.
- Work with IT Manager and IT Team for procurement of new and reoccurring services which are in place to facilitate Cyber Security measures.
- Work with IT Manager to maintain Chief Information Security Officer service provision and build good relationship with CISO ensuring Cyber Security trends are managed appropriately.

### Work with Information Officers to provide an Information Security Function

- Review existing policies & procedures of the Information Services Team and ensure information security considerations are included and implemented.
- Input and Review existing Information Risk Register with Cyber Security in mind.
- Undertake routine Business Impact Assessments of SEUPBs Information Assets, updating the Information Asset Registry as required.
- Provide a liaison point for DPO and CISO external service providers when implementing information security best practices.

### Cyber & Information Security Training Support for SEUPB staff

- Work with SMET, IT and HR teams to put in place a bespoke training programme around Cyber Security which is closely related to SEUPB IT Estate, also ensure new staff are trained on Cyber Security.

### Keep abreast of new Cyber Security Threats

- Setup relationships with relevant Cyber Security organisations, e.g. CISO, Incident Management Team, NCSC, NICSC, PSNI Cyber Security, Gardai Cyber Branch.
- Ensure SEUPB is up to speed with all latest trends of Cyber Security threats, establish links with relevant bodies and organisations to ensure SEUPB is aware of new developments to enable speedy mitigation measures.

### Build solid partnerships with external service providers e.g. CISO

- Work with IT Manager to maintain Chief Information Security Officer service provision and build good relationship with CISO ensuring Cyber Security trends are managed appropriately.
- Work with IT Manager, Information Services team and Records Management Managed Service provider to ensure there is an effective DPO as a service provision for SEUPB and build a strong relationship with external DPO ensuring all SEUPB Information Assets are managed sensitively and securely.
- Work closely and maintain good working relationships with existing IT Service Providers to ensure SEUPB is sufficiently protected from Cyber Threats.
- Manage a Security Testing contract to ensure areas identified in Cyber Security Maturity Assessment are routinely tested from both external and internal threat actors. Provide input to setting up and management of an Incident Response Contract.

### Develop reports for IT Manager and SMET (Senior Management Exec Team)

- Use a variety of exiting information sources to provide both detailed and high-level reports on the SEUPB IT and Information Asset Estate to present to the IT Manager and SMET team.

- Continuously review and seek out new information sources to ensure up-to-date issues or risks are identified within reports so that mitigations can be taken

**The above is given as a broad range of duties and is not intended to be a complete description of all tasks.**

# PERSON SPECIFICATION

**JOB TITLE:**
IT Security Officer (Belfast Based) 3 Year Fixed -Term Contract

**HOURS:**
Minimum 37 hours per week (excluding breaks)

**SALARY SCALE:** £32,880 to £34,011 (Under Review)

**REPORTS TO:**
IT Manager

**LOCATION:**
The successful candidates will be based at the Clarence West Building, Clarence West Street, Belfast BT2 7GP.

**ESSENTIAL CRITERIA and QUALIFICATIONS:**

- A minimum of Higher National Diploma or Degree level qualification in an IT related discipline
- Minimum - CompTIA Security+ certification (or higher security certification))
- 5 GCSEs grades A-C (including English Language and
- Maths) or equivalent
  or
- Leaving Certificate – 5 grades A-C (including English Language and Maths) or equivalent.

**DURATION OF APPOINTMENT**

This is a 3-year fixed term contract from date of appointment.

**EXPERIENCE:**

- Experience in ensuring organisation is up to speed with evolving Cyber Threats and mitigations.
- Experience in work in partnership with IT to manage implementation of Threat Vulnerability Management (TVM) process, ensuring system risks are considered, remediation where needed is carried out, and all actions logged.
- Experience in dissecting a large volume of source data from systems and portals to be able to draft monthly reports/dashboards on IT Security Posture for a non-technical audience.
- Experience with investigations in suspected and actual cyber security incidents in accordance with appropriate Cyber Security incident management response plan, and ensure any remedial action were taken.
- Experience gained in providing organisations with Information Management security advice to ensure safety of all information (Personal and Sensitive) is realised at all times, and compliance with such information adhered to.

- Experience in bottom-up review of all Information Technology and Information Management policies to ensure policies are fit for purpose and meet updated regulatory compliance requirements, updating policies where necessary.
- Experience gained in putting in place a programme of regular reviews of policies which impact an IT and IM team, and indeed organisationally.
- Experience gained in building relationships with expert IT security service providers (e.g., CISO) and other professional bodies (e.g., NICSC).
- Experience gained in providing an IT Security specific advisory function to the existing IT Team on all matters relating to cyber security.
- Experience gained in providing routine training to an organisation either directly or via a training partner on Cyber Security to improve staff awareness on all types of threats

## REQUIRED COMPETENCIES

### Seeing the Big Picture

- Seek to understand how the services, activities, and strategies work together in the business area to create value for the customer/end user.
- Contribute to the development of policies, plans and service provision to meet citizens' diverse needs based on an up-to-date knowledge of needs, issues, and relevant good practice.

### Changing and Improving

- Find ways to improve systems, policy development and structures to deliver with more streamlined resources.
- Regularly review procedures or systems with teams to identify improvements and simplify processes and decision making.
- Drive lessons learned from incidents to improve SEUPB Security Measures.

### Making Effective Decisions

- Make decisions when they are needed, even if they prove difficult or unpopular.
- Recognise patterns and trends in a wide range of evidence/data that may affect policy and draw key conclusions.
- Invite challenge and, where appropriate, involve others in decision making to help build engagement and present robust recommendations.

### Building Capability for All

- Identify and address team or individual capability requirements and gaps to deliver current and future work.
- Develop team members, devoting time to coach, mentor and develop others.
- Proactively manage own career and identify own learning needs with line manager, plan and carry out workplace learning opportunities.

### Managing a Quality Service

- Make effective use of project management skills and techniques to deliver outcomes, including identifying risks and mitigating actions.
- Develop, implement, maintain, and review systems and service standards to provide quality, efficiency, and value for money.
- Promote a culture that tackles fraud and error, keeping others informed of outcomes.
- Establish mechanisms to seek out and respond to feedback from customers about policy and service provided.

### Delivering at Pace

- Successfully manage, support, and stretch self and team to deliver agreed goals and objectives.
- Take responsibility for delivering expected outcomes on time and to standard, giving credit to terms and individuals as appropriate.

### Achieving Outcomes through Delivery Partners

- Work with experts in engaging effectively and intelligently with delivery partners in order to define and/or improve policy and service delivery.
- Consider, in consultation with experts, alternative ways of working with partners and contractors to identify more efficient outcomes, balancing cost, quality and turnaround times.

## DESIRABLE CRITERIA and QUALIFICATIONS

These will be used for shortlisting purposes in the event of a large number of applicants.

### EXPERIENCE

- Experience (or understanding) of firewalls, SIEM, SOC, Proxies, Antivirus, IDPS, XDR would be an advantage.
- Experience of developing and implementation of supply chain security frameworks.
- Experience with assisting an
- Organisation(s) achieve Cyber Essentials / Cyber Essentials Plus certification.
- Experience with assisting an organisation(s) obtain ISO 27001 Information Security Standard certification.

### REQUIREMENTS

- Travel will be required occasionally to visit each of the office locations in Northern Ireland and Ireland.

# WHAT WE OFFER

### Blended (Hybrid) Working
SEUPB offers a blended working arrangement based on three days in the office and two days homeworking per week. This facility will be applicable to this role after two months, following full completion of onboarding, training, and familiarisation.

### Financial
To attract, motivate and retain talented people we believe an attractive, flexible and rewarding pay structure is essential. (We therefore offer our employees competitive salaries).

### Pension
The SEUPB operates a defined benefit occupational pension scheme (the North South Pension Scheme) worked out on a Career Average basis.
We have outlined some of the key features of the Scheme below.

Generous pension payable for life after you retire which increases in line with inflation*
The pension amount is based on your average salary during your career and the number of years you spend in employment.

The best way to think about the value of the pension is to estimate how much you might have to save to get an equivalent pension privately via another pension scheme. For illustration purposes, as a % of your pay, the cost of an equivalent pension might be up to 40% of pay per year. This annual cost increases with age (i.e. the older you are the greater the % of pay it costs to pay for your pension). So, you'd have to put a significant proportion of your earned income aside to secure such a pension.

As it turns out, typically you are required to make a contribution of between 4.6% and 7.35% of pay per year, with the balance effectively funded by the Northern Ireland Executive and the Irish government. There are other benefits payable too to provide protection to you and any beneficiaries in the event of illness or death.

*Inflation is measured by an index known as the Consumer Price Index (CPI) which measures changes in the price level of a weighted average market basket of consumer goods and services purchased by households.

### Holidays NI
We offer our staff an annual leave entitlement of 25 days rising to 30 days after 5 years' service. In addition to this we also offer 12 statutory holiday days.

### Employment Policies
The SEUPB recognises the importance of work life balance and offers a range of family friendly policies and practices for its employees.

### Learning and Development
All employees will have access to the SEUPB Employee Support & Development Programme. The SEUPB has a dedicated Learning and Development Strategy in which we provide our employees with the training they need to be as efficient and productive while also offering development opportunities to further develop their career in the SEUPB.

### Cycle to Work Scheme
You are encouraged to take advantage of our 'Cycle to Work' scheme, which gives you access to a bike and equipment valued to £1,000 through a VAT-free scheme, for use commuting to and from work.

### Family Leave
Maternity Leave – Up to 52 weeks of which 18 weeks is on full pay. We also offer Paternity Leave, Parental Leave/Shared Parental Leave and Adoption Leave.

### Healthcare
All employees of the SEUPB and their families and friends are eligible to join a private healthcare scheme which provides a range of healthcare services on a discretionary basis at a low monthly cost.

### Employee Assistance Programme
All our employees have access to a fully independent 24-hour helpline to assist with any of life's issues or problems, along with access to an accredited counselling service. (All of which is free at the point of use and completely confidential).

### Location
The SEUPB Headquarters is located in Belfast with two Regional Offices in Monaghan and Omagh.

## EQUALITY STATEMENT

SEUPB is committed to equality of opportunity and welcomes applications from suitably qualified candidates irrespective of religious belief, gender, disability, race, political opinion, age, marital status, sexual orientation, or whether or not they have dependants.

*The Body would particularly welcome applications from the Protestant community who are currently under-represented in the workforce.*

# THE SELECTION PROCESS

### Eligibility Sift

Shortlisting of candidates on the basis of the information contained in their application.

### Completing the Application Form

Those candidates who are invited for interview who had submitted their application electronically will be required to formally sign their applications prior to being appointed.

All applications must be made on the form supplied by the SEUPB. (CVs will not be accepted).

Under each of the headings in the application form, candidates are asked to provide a clear and relevant example drawn from their recent work, which illustrates how they match the competence being sought. The information on the application form will be used for sifting and only those candidates who can meet all of the Essential Criteria will be considered for interview.

### Shortlisting

The first stage in the selection process will be to conduct a sift of completed application forms against the essential qualification criteria. Applicants who have not fully demonstrated on their application form how they meet this criterion will not be progressed to the next stage of the process.

Application forms are formatted so that applicants are required to demonstrate how they meet each essential competency. The onus will be on applicants who are completing application forms to demonstrate how they meet each competency.

Where a specified period of experience is mentioned, it may be increased by one-year increments as a method of reducing numbers.

Applications will also be considered from applicants with relevant formal qualifications considered by the selection panel to be of an equivalent or higher standard to those stated above. If putting forward an equivalent qualification, please provide the type of qualification and date awarded. The date awarded is the date on which you were notified of your result by the official awarding body. If you believe your qualification is equivalent to the one required, the onus is on you to provide the panel with details of modules studied etc. so that a well-informed decision can be made.

Should the SEUPB receive a high level of applications, the desirable criteria may be applied to shortlist candidates for interview. Additionally, a short Microsoft Excel exercise may be included as part of the assessment process for this role.

### At the interview

Those candidates called for interview will be questioned on the areas covered in the application form, personnel specification, and job description. Candidates will be asked questions to enable them to illustrate their competence in each of the areas. They may enlarge upon the information provided on the application form or use different information to illustrate the answer. Candidates will be assessed against the essential criteria and key competencies identified as being a requirement for the role.

## ADDITIONAL INFORMATION

Applicants should note that starting salary would normally be at the minimum of the pay scale.

Applicants who intend to return their applications by post should ensure that they post documents in sufficient time to reach us by the closing date 9.00am 18th September 2023

Late applications will not be accepted under any circumstances. We will accept application forms by either post or electronically by the closing date and time. It is your responsibility to ensure applications reach us by the notified deadline.