Risk Assessment Procedure

St Peter's, Colchester

Adopted by the PCC: [tbc]

Review date: [3 years]

Policy owner: The Parochial Church Council

---

1. Purpose

This procedure explains how risk assessments are identified, completed, checked, shared, reviewed and stored at St Peter's.

The PCC has responsibility for the governance and oversight of St Peter's, including risk management, safeguarding, health and safety, fire safety, buildings, finance, staff, volunteers and church activities.

As disciples of Jesus Christ, we seek to be faithful in all that we say and do. That includes taking reasonable care of one another, protecting the vulnerable, stewarding resources wisely, and ensuring that ministry is carried out in a safe, responsible and well-ordered way.

This procedure is intended to make risk assessment practical, clear and proportionate, so that risk management supports ministry rather than becoming an unnecessary burden.

2. Scope

This procedure applies to risk assessments connected with the life, ministry, buildings and activities of St Peter's.

This may include:

- worship services;
- children's and youth ministry;
- pastoral care and visiting;
- church office and administration;
- church building, hall, churchyard and premises;
- health and safety;
- fire safety;
- food and hospitality;
- events, courses, groups and outreach activities;
- external hire and use of premises;
- lone working;
- manual handling;

- cleaning, maintenance and practical tasks;
- trips, visits and off-site activities;
- data, IT and communications where relevant;
- safeguarding-related risks;
- other activities or responsibilities carried out on behalf of St Peter's.

This procedure applies, as relevant, to:

- PCC members;
- the Vicar;
- churchwardens;
- employed staff;
- Ministry Area Leaders;
- safeguarding officers and teams;
- volunteers;
- event organisers;
- those responsible for premises, groups, activities or ministries.

3. Relationship with the Governance and Risk Management Policy

The Governance and Risk Management Policy sets out St Peter's overall approach to governance, risk oversight, the Risk Register, risk analysis, operational controls, reporting and review.

This procedure explains how ordinary risk assessments should be handled in practice.

Risk assessments are one part of St Peter's wider risk management framework. They should be used alongside:

- the Risk Register or risk analysis;
- PCC policies;
- safeguarding procedures;
- fire safety arrangements;
- health and safety procedures;
- action plans;
- incident reporting;
- Ministry Role Descriptions;
- training and supervision;
- relevant Church of England, diocesan, statutory or professional guidance.

4. Principles

Risk assessment at St Peter's should be:

- proportionate to the activity and level of risk;

- practical and usable;
- clear enough for staff and volunteers to follow;
- focused on real risks, not theoretical paperwork;
- consistent with safeguarding requirements;
- reviewed when circumstances change;
- stored in an organised way;
- shared with those who need to know;
- escalated where risk cannot be managed locally.

Risk assessment should not normally prevent ministry, hospitality, pastoral care, children's work, outreach or church activity. Its purpose is to help those things happen wisely, safely and responsibly.

5. When a risk assessment is needed

A risk assessment should normally be completed or reviewed when:

- a new ministry, activity, group or event begins;
- an existing activity changes significantly;
- an activity involves children, young people or vulnerable adults;
- an activity involves food, travel, off-site work, lone working, manual handling, equipment, cash, keys, buildings, fire safety, public access, external visitors or safeguarding risks;
- an event is unusual, large, complex or outside normal church routines;
- a building, room, storage area, churchyard or premises arrangement changes;
- there has been an accident, incident, near miss, complaint or safeguarding concern;
- a previous risk assessment is due for review;
- guidance, law, insurance requirements, diocesan advice or PCC policy changes;
- someone with responsibility identifies a significant risk.

Not every small or ordinary activity needs a separate written risk assessment if it is already covered by an existing current risk assessment. However, those responsible for an activity should still consider whether anything has changed or whether additional precautions are needed.

6. Responsibility for ensuring risk assessments are completed

The person responsible for a ministry area, activity, event or area of work is normally responsible for ensuring that an appropriate risk assessment is completed or reviewed.

This may be:

- the Ministry Area Leader;
- the event organiser;
- the member of staff responsible for the activity;
- the Vicar;
- a churchwarden;

- the Church Administrator;
- the Safeguarding Team;
- the Buildings, Fabric and Development lead or group;
- the Health and Safety lead or group;
- another person or group delegated by the PCC.

For regular ministries, the relevant Ministry Area Leader should normally ensure that relevant risk assessments are in place, current, understood and followed.

The PCC retains overall responsibility for ensuring that risk management arrangements are adequate. PCC members, or delegated PCC representatives, may therefore need to check that risk assessments have been completed and reviewed.

7. Who should complete a risk assessment?

A risk assessment should normally be completed by someone who understands the activity, setting or ministry being assessed.

Where needed, they should consult others, such as:

- staff or volunteers involved in the activity;
- the Vicar;
- churchwardens;
- the Church Administrator;
- the Parish Safeguarding Officer;
- children's or youth leaders;
- buildings or maintenance leads;
- health and safety or fire safety leads;
- those with relevant professional expertise;
- diocesan or external advisers.

Where an activity involves safeguarding, children, young people or vulnerable adults, the risk assessment must be consistent with St Peter's Safeguarding Policy and should involve appropriate safeguarding input.

Where an activity involves buildings, fire safety, food, manual handling, maintenance or technical risks, appropriate practical or specialist advice should be sought where needed.

8. What a risk assessment should include

A risk assessment should normally identify:

- the activity, event, location or ministry being assessed;
- the person completing the assessment;
- the date completed;
- the review date;
- who may be harmed or affected;
- the main hazards or risks;

- the possible consequences;
- existing control measures;
- additional actions needed;
- who is responsible for those actions;
- when actions should be completed;
- whether the remaining risk is acceptable;
- who prepared, reviewed and approved the assessment.

The level of detail should be proportionate to the risk. A simple activity may need only a short assessment. A higher-risk, new, unusual, safeguarding-related or public activity may need a more detailed assessment.

9. Checking and approval

Risk assessments should identify the following three roles:

1. "Prepared by" – the person who drafts or completes the risk assessment;
2. "Reviewed by" – a suitable person who checks the assessment for completeness, proportionality, clarity and any significant omissions;
3. "Approved by" – the Ministry Area Leader, activity leader, event organiser or other person who holds responsibility for the activity and for ensuring that the identified control measures are implemented.

The person preparing the assessment may also be the person responsible for the activity. However, wherever reasonably practicable, the person reviewing the assessment should be someone other than the person who prepared it.

For routine or lower-risk activities, the review may be undertaken by an appropriate staff member, Church Administrator, safeguarding officer, Health and Safety Officer, churchwarden or another person with suitable knowledge of the activity.

For higher-risk, unusual or more significant activities, the assessment should be reviewed by an appropriate responsible person or group. This may include:

- the Vicar;
- the churchwardens;
- the Church Administrator;
- the Parish Safeguarding Officer or Safeguarding Team;
- the Health and Safety Officer;
- the relevant Governance Group;
- Standing Committee;
- or the PCC.

Approval should be given only when the approver is satisfied that the significant risks have been identified, that the control measures are proportionate and workable, and that responsibility for implementing them is clear.

Where an assessment identifies a significant unresolved risk, a need for substantial expenditure, a safeguarding concern, a legal or insurance issue, or a matter outside the authority or competence of the activity leader, it must be escalated before the activity proceeds.

10. Sharing risk assessment information

Relevant risk assessment information must be shared with those who need to know it.

This may include:

- staff;
- volunteers;
- Ministry Area Leaders;
- event organisers;
- children's and youth leaders;
- pastoral visitors;
- welcome teams;
- wardens;
- safeguarding officers;
- building users;
- external hirers where relevant;
- contractors where relevant.

It is not always necessary to share the whole risk assessment with everyone. In many cases, the key control measures, practical instructions and relevant actions are what need to be communicated.

Those responsible for an activity should ensure that volunteers and helpers know:

- what the main risks are;
- what precautions must be followed;
- what to do in an emergency;
- who to contact if there is a concern;
- what must be reported afterwards.

Where safeguarding-related information is involved, it should be shared only as necessary and in accordance with safeguarding and data protection requirements.

11. Review

Risk assessments should be reviewed:

- by the review date stated on the assessment;
- when an activity changes;
- when the people involved change significantly;
- when a room, building or layout changes;
- after an accident, incident, near miss, safeguarding concern or complaint;
- when guidance, policy, law or insurance requirements change;

- when a responsible person identifies that the assessment may no longer be accurate;
- before repeating an event where previous arrangements may no longer be suitable.

For regular activities, review dates should be realistic and proportionate. A standard annual review may be appropriate for many operational risk assessments, while higher-risk areas may need more frequent review.

A risk assessment should not simply be copied forward without checking whether it still reflects current practice.

12. Actions arising from risk assessments

Where a risk assessment identifies actions, those actions should be recorded and followed up.

Actions should normally state:

- what needs to be done;
- who is responsible;
- by when;
- whether the action is urgent;
- whether the activity can proceed before the action is completed;
- when the action has been completed.

Where actions are significant, unresolved or beyond the authority of the activity leader, they should be escalated to the appropriate person or group.

Actions may need to be included in:

- an activity action list;
- a ministry area plan;
- a buildings or maintenance action plan;
- a safeguarding action plan;
- a health and safety action plan;
- the Risk Register;
- PCC or Standing Committee papers;
- another compliance or operational action plan.

13. Escalation

Risks should be escalated promptly where they involve:

- safeguarding concerns;
- serious risk of harm;
- fire safety;
- unsafe buildings, equipment or premises;
- significant health and safety concern;
- possible abuse, coercion, bullying or harassment;
- unresolved volunteer or staffing concerns;

- serious financial, legal or insurance implications;
- data breach or cyber security risk;
- reputational risk;
- repeated incidents or near misses;
- risk that cannot be managed by the activity leader;
- refusal or failure to follow agreed safety measures.

Escalation may be to:

- the Vicar;
- the churchwardens;
- the Church Administrator;
- the Parish Safeguarding Officer;
- the Safeguarding Team;
- the Health and Safety lead or group;
- the Fire Safety lead or group;
- the Buildings, Fabric and Development group;
- Standing Committee;
- the PCC;
- diocesan or external advisers;
- emergency services where required.

In an emergency, immediate action should be taken to protect people and property. The matter should then be reported afterwards to the appropriate person or body.

14. Safeguarding-related risk assessments

Risk assessments involving children, young people, vulnerable adults, pastoral care, known vulnerability, allegations, concerning behaviour, domestic abuse, sexualised behaviour, one-to-one contact, transport, overnight activity, online contact or safeguarding concerns must be aligned with St Peter's Safeguarding Policy.

Safeguarding-related risk assessments may need input from:

- the Parish Safeguarding Officer;
- the Safeguarding Team;
- the Vicar;
- diocesan safeguarding advisers;
- relevant statutory agencies;
- Thirtyone:eight or other safeguarding advisers where appropriate.

Safeguarding-related risk assessments should be handled with appropriate confidentiality. They should not be stored in ordinary shared folders or circulated more widely than necessary.

Where safeguarding risk is present, safeguarding procedures take priority. A safeguarding concern must not be treated merely as an ordinary operational risk.

15. Storage and document control

Current risk assessments should be stored in the agreed St Peter's risk assessment folder or document-control system.

Risk assessments should be clearly named and dated.

Where possible, the file name or document should identify:

- ministry, activity or location;
- date completed or reviewed;
- review date;
- current status.

Superseded risk assessments should normally be archived rather than deleted, especially where they relate to safeguarding, children's work, youth work, pastoral care, buildings, fire safety, accidents, incidents, complaints, external hire, insurance, employment, volunteers or legal responsibilities.

Drafts, working copies and duplicate versions should be managed carefully so that staff and volunteers know which version is current.

16. Records of incidents, concerns and near misses

Incidents, accidents, near misses, safeguarding concerns, complaints, property damage, fire safety issues, aggressive incidents, data breaches, lost keys, injuries or other significant concerns should be recorded and reported through the relevant process.

Such reports should be considered when reviewing risk assessments.

Repeated minor concerns may indicate a more significant risk and should not be ignored.

17. Training and support

Those responsible for activities, events, ministries or areas of work should be given appropriate guidance and support so that they understand how to complete and use risk assessments.

Training or support may be provided through:

- induction;
- Ministry Role Descriptions;
- staff or volunteer meetings;
- safeguarding training;
- health and safety guidance;
- written templates;
- example risk assessments;
- support from the Church Administrator, Vicar, churchwardens, safeguarding officers or governance groups.

Risk assessment should be treated as part of ordinary ministry planning and good stewardship, not as a specialist task only understood by a few people.

18. Related policies and documents

This procedure should be read alongside, where applicable:

- Governance and Risk Management Policy;
- Risk Register;
- Safeguarding Policy;
- Safer Recruitment arrangements;
- Health and Safety Policy;
- Fire Risk Assessment;
- Fire Evacuation Plans;
- Fire RA Action Plan;
- Lone Worker Policy;
- Manual Handling Policy;
- Food Hygiene Policy;
- Buildings, Fabric and Development documents;
- Volunteer Policy;
- Volunteer Agreement;
- Ministry Role Descriptions;
- Code of Conduct;
- Complaints Policy;
- Whistleblowing Policy;
- Data Protection Policy;
- Privacy Notice;
- Data Retention Policy;
- IT Security Policy;
- Staff Handbook and employment policies;
- relevant Church of England, diocesan, insurer, statutory or professional guidance.

19. Review

This procedure will be reviewed every three years, or sooner if required by changes in law, Church of England guidance, diocesan guidance, safeguarding requirements, health and safety requirements, parish practice, insurance requirements, incidents or governance need.

Individual risk assessments may need to be reviewed more frequently, depending on the activity, risk level, review date, incident history or changes in circumstances.

The PCC is responsible for ensuring that this procedure remains practical, proportionate and consistent with St Peter's wider governance and risk management framework.

Short public-facing summary

Risk Assessment Procedure

St Peter's uses risk assessments to help church life happen wisely, safely and responsibly.

Risk assessments may be needed for ministries, events, children's and youth work, pastoral care, buildings, food, fire safety, lone working, trips, practical tasks, external hire and other church activities.

The person responsible for a ministry, event, activity or area of work should normally ensure that an appropriate risk assessment is completed or reviewed. For regular ministries, this will usually be the relevant Ministry Area Leader.

Risk assessments should identify the main risks, who may be affected, what precautions are in place, what actions are needed, who is responsible, and when the assessment should be reviewed.

Relevant information from risk assessments should be shared with those who need to know it, including staff, volunteers and activity leaders.

Safeguarding-related risk assessments must be consistent with St Peter's Safeguarding Policy and handled with appropriate confidentiality.

Risk assessments should be reviewed when activities change, after incidents or concerns, and by their review date. Current assessments should be stored clearly, and superseded versions should normally be archived rather than deleted.