## Appendix 1: Areas of Risk

The following table provides details of operational areas that are particularly susceptible to fraud, and identifies controls that should be in place.

| Area of Risk | Controls |
|---|---|
| Theft | • Cash, cheques, electronic equipment and other valuable items should be held securely at all times.<br>• Access to cash should be restricted to named personnel.<br>• Keys should only be issued to authorised personnel.<br>• Cash balances should be regularly recorded and checked, and kept to a minimum where possible. |
| Updates to accounting records | • Amendments to accounting records should be independently authorised and accompanied by the relevant signature, name, position, and authorisation code (if applicable).<br>• All amendments should be independently verified.<br>• All amendments should leave the original figure legible.<br>• Accounting records and petty cash should be reviewed on a regular basis, with any discrepancies being promptly investigated.<br>• Suspense accounts should be reviewed on a regular basis. |
| Invoices | • There tasks of processing and authorising invoices should be separate and independent.<br>• Checks for duplicate invoices should be carried out regularly.<br>• Invoices should be crossed referenced with orders to ensure their validity and accuracy. |
| Expenses and Reimbursement | • Authorising officers should ensure that expenses and other claims are claimed at the correct rate.<br>• Receipts and invoices should be retained in support of every claim.<br>• Authorising officers should prevent duplicate claims by comparing the GPC return and the T&S return.<br>• All new GPC cards should be sent to the GPC Administrator for distribution, and sent via secure DX or recorded delivery.<br>• GPC holders should receive training at the point of issue.<br>• National Office Finance Team should regularly analyse expenditure. |
| Breaches and loss of official information | • Paper documents should be securely stored away when not in use.<br>• Electronic information should be stored on Cafcass issued encrypted devices, and securely backed up.<br>• Managers should ensure that access to particularly sensitive information is restricted to authorised persons. |