

Reviewed: September 2023

Charging Policy

Introduction

This charging policy has been compiled in line with DFE requirements, North Northants Council provider agreement and in accordance with s457 of the Education Act, 1996.

At the Integrated Centre the Joint Heads of Centre, the Finance Manager and the Centre Leaders work together to manage the Integrated Centre's budgets. They will make recommendations to the Governor's Finance, Personnel and Resources Committee on the levels of charges to be made for all services in the Centres. All charges levied will be to ensure the Centre meets the costs of additional services offered.

Additional Hours of Childcare over and above the funded hours.

All funded entitlement is free at the point of deliver but we will make charges for any additional hours taken up by parents or carers over and above the funded entitlements. All additional costs are detailed and published on our offer. Parents/carers will be contracted to pay 2 weeks in advance for costs for any additional hours required.

Meals, consumables and snacks

Government funding is intended to deliver 15 or 30 hours a week, over 38 weeks of the year, high quality, flexible childcare. It is not intended to cover the costs of meals, snacks, other consumables, additional hours or additional activities. Parents can therefore expect to pay for any consumables including meals and snacks offered by the Integrated Centre. Cost of meals and consumables will be invoiced separately from additional hours and services.

Centre Outings

Integrated Centre outings where children go with Family Workers to local areas of interest or family outings where parents are encouraged to accompany their children and join in the learning experience. Where these are curriculum-based trips, the Integrated Centre will endeavour to cover all or part of the cost of the children's transport and activity/entrance fees. Parents may be asked for a contribution to cover some of the cost for their children. Parents will be asked to cover the cost of their own transport and activities/entrance fees on these days. Where insufficient contributions are received outings may have to be cancelled.

Damage/Loss to Property

A charge will be levied in respect of wilful damage, neglect or loss of Integrated Centre's property or property belonging to a third party where the cost has been recharged (including premises, furniture, equipment, books or materials). The charge will be the cost of replacement or repair, or such lower cost as the Joint Heads of Centre may decide.

Lettings

The Integrated Centre will make its facilities available to outside users at a charge of at least the cost of providing the facilities, the Integrated Centre policy is aligned to the Local Authority lettings policy. The scale of charges will be determined by the Finance Committee.

Visitor days, conferences and short courses

The integrated Centre will offer learning and development activities. Delegates will be charged in advance. In the event of non-payment, we reserve the right not to accept future bookings and cancel existing bookings until outstanding amounts have been paid in full.

If you or your organisation cancel your place you will be charged at the published rate if you give 10 or less working days' notice for cancellation. If you fail to attend an activity on which you are booked, then the fees will be payable in full.

We reserve the right to cancel an activity, giving as much notice as possible if events arise beyond our control which makes delivery of the learning and development activity impractical. We will endeavour to offer alternative arrangements.

Additional charges

The Joint Heads of Centre, Finance Committee or Governing Body may levy charges for miscellaneous services up to the cost of providing such services e.g., for providing a copy of a publication or journal article.

Universal entitlement

From the term following a child's third birthday parents are entitled to a maximum of 570 hours funded childcare per year. This is spread across three funding blocks, with a maximum of 15 hours a week. No charge will be levied for parents claiming their funded entitlement only.

The **Pen Green Centre** offers the Universal entitlement at 15 hours per week during term time only over 38 weeks per year either in the morning between 8.45am and 11.45am or in the afternoon between 12.30pm and 3.30pm. Alternatively, at 12.5 hours per week year-round excluding summer closure, Christmas closure and bank holidays either in the morning between 9.15am and 11.45am or in the afternoon between 1.00pm and 3.30pm

The **Kingswood Community Nursery** offers the Universal entitlement at 15 hours per week during term time only over 38 weeks per year either in the morning between 9am and 12pm or in the afternoon between 1pm and 4pm.

Parents can request additional childcare hours outside the universal funded sessions at a charge. Please see offer structure attached to Pen Green Additional Hours Contract. Parents may claim their entitlement from more than one provider at the same time but may not exceed 570 hours over 3 funding periods.

Where parents have claimed at a different setting the Integrated Centre reserve the right to charge the parent for any funding shortfall for their child, at the rate of universal funding paid by North Northants Council.

Extended entitlement

Some parents and carers of three and four year olds may also be eligible to claim for extended hours up to 1140 hours a year, spread across three funding blocks.

The Pen Green Centre offers the Extended entitlement over 25 hours per week year round, excluding summer closure, Christmas closure and bank holidays. The extended entitlement is offered between 9.00am and 2.00pm or 1pm – 6pm. Any additional childcare hours required outside of these extended funded hours will be charged.

The **Kingswood Community Nursery** offers the extended entitlement over 30 hours over 38 weeks per year. The extended entitlement is offered between 9am and 3pm.

2 Year olds

From the term following a child's second birthday parents in receipt of certain benefits may be entitled to a maximum of 570 hours funded childcare per year. This is spread across three funding blocks, with a maximum of 15 hours a week over 38 weeks per year.

The Pen Green Centre offers the 2-year-old entitlement at 12.5 hours per week year-round excluding summer closure, Christmas closure and bank holidays either in the morning between 9am and 11.30am or in the afternoon between 1.00pm and 3.30pm.

The **Kingswood Community Nursery** offers 15 hours per week during term time only over 38 weeks per year either in the morning between 9am and 12pm or in the afternoon between 1pm and 4pm.

Where parents have claimed at a different setting, the Integrated Centre reserve the right to charge the parent for any funding shortfall for their child at the rate of the 2-year-old entitlement funding paid by North Northants Council.

Remissions Policy

A child may be eligible for the Early Years Pupil Premium if their parents are in receipt of one of the following:

- Income Support
- Income-based Jobseekers Allowance
- Income-related Employment and Support Allowance
- Support under Part VI of the Immigration and Asylum Act 1999
- The guaranteed element of State Pension Credit
- Child Tax Credit

- Working Tax Credit run-on – paid for 4 weeks after you stop qualifying for Working Tax Credit.

A separate policy outlines the use of the **Early Years Pupil Premium** however charges in respect of outings will be remitted in full for children in receipt of pupil premium.

The Joint Heads of Centre, Finance, Personnel and Resources Committee or Governing Body may remit in full or part charges in respect of any child, if it feels it is reasonable in the circumstances.

The Joint Heads of Centre, Finance, Personnel and Resources Committee or Governing Body may decide not to levy charges in respect of a particular activity, if it feels it is reasonable in the circumstances.

Annual Review of Charges

The Finance, Personnel and Resources Committee will review charges on an annual basis. Wherever possible where changes to the charges have been made these will come into effect in the September of that year; where funding levels change at the beginning of the financial year this may not always be possible.

Student Fees

In relation to student fees each course that is held within the Research, Development and Training Base has its own payment structure specific to Student Finance England. For more information on the scale of charges please contact the Senior Finance Officer on 01536 443435.

Levy of Charges

Parents of children within the Integrated Centre will be invoiced every week for meals and any additional childcare sessions over and above their funded entitlement. Charges made to parents/carers for any additional services or hours of childcare over and above the funded hours will be clearly explained and itemised on invoices.

Invoices will be in accordance with your Pen Green/Kingswood Childcare Contract/Nursery Contract. Parents will be charged full fees for child's sickness, personal holidays, bank holidays, closure over the Christmas and New Year period, and up to 5 staff training days per year and for unplanned centre closure due to adverse weather. There will be no charge for food when on annual holidays.

We strive to be a cashless organisation and parents are asked to pay these invoices on a weekly or monthly basis by either setting up a standing order, by making an on-line banking transfer or by using the Chip and PIN facility available in reception.

When a payment is not made, parents must meet with a member of the finance team to negotiate a payment plan. If the payment plan is not adhered to, possible actions may range from immediate

withdrawal of the additional hours offered to agreement and that siblings who attend the Integrated Centre in the future will not be offered the opportunity to increase their hours beyond

their funded entitlement. This is to ensure that parents do not get themselves further into debt. Please also refer to the Debt Recovery policy.

Aged debtor reports will be presented, and possible actions discussed and agreed at the Finance, Personnel and Resources Committee on a termly basis.

Reviewed September 2023

Debt Recovery Policy

Policy Intention

The intention of this policy is to achieve the prompt collection of all sums of money due to the Centre, whilst ensuring that a fair and consistent approach is taken to the recovery of sums that are not paid when due.

Commencement and Duration

This Policy shall take effect from 1 September 2021. The Policy will have continuous effect but shall be reviewed from time to time, as required. A review of the Policy shall be conducted at least once every five years.

Debt recovery process

Parents of children within the Integrated Centres will be invoiced every week for additional childcare sessions over and above their funded entitlement. We are a cashless organisation and parents are encouraged to pay these invoices on a weekly or monthly basis by either setting up a standing order, by making an on-line banking transfer or by using the Chip and PIN facility available in reception.

Weekly aged debtor reports are prepared and presented to the leads for each nursery space. Any non-payment of invoices will be identified at this stage. A monthly statement will be issued to parents with outstanding balances mid-month and the end of the month.

A member of the finance team will often be available in reception in the morning if you have any queries re your invoice or a meeting can be arranged by request.

Initial reminders

Initial reminders may be informal and made either in person when the parent comes to collect/drop off their child or by telephone by a member of the finance team.

First reminder letter

If payment is not received within 4 weeks from the invoice due date, and no request is received to consider a payment plan, a first reminder letter will be sent. At this stage we will have to consider whether we can continue to offer your child any sessions over and above their funded entitlement.

Second reminder letter

A second reminder letter will be sent 4 weeks after the first reminder letter, either electronically or by post. This letter will only be sent out with authorisation from the family worker/ head of domain and after a discussion to include:

- An accurate history of the origin of the debt and of the attempts made to recover it,
- Details of any other debts owed to the Centre by the same debtor,
- Information about any other disputes in respect of the debt,
- An assessment of the prospects of recovering the debt by other means in reasonable timescale,
- Consideration of whether the debtor's personal circumstances warrant them being protected from the consequences of recovery action,
- Details of attempts made to contact the debtor and of the outcome of the attempts.

Failure to respond to reminders/settle a debt

If no response is received from the reminders issued, a letter will be sent to the parent/carer advising them that the matter will be referred to either

- The Centre's approved collection agent, or
- Be pursued through a claim through the Small Claims Court.

Cost of debt recovery

Where the Integrated Centres incur material additional costs in recovering a debt then the Finance Committee will decide whether to seek to recover such costs from the parent/carer. The parent/carer will be formally advised that they will be required to pay the additional costs incurred by the Integrated Centres in recovering the debt.

Reporting of outstanding debts

The finance manager will ensure that the level of outstanding debt is known and can be determined at any time. An aged debtors report will be discussed at Governors meetings and the write off of any debt requires the written approval of the Chair of the Finance and Personnel Committee and the Chair of Governors.

Reviewed September 2023

Electronic Financial Security Policy

Introduction

This Policy Document encompasses all aspects of security surrounding confidential financial information and must be distributed to all staff who are involved in the use of the organisation's electronic financial systems (Chip & Pin machines, including remote use where the customer is not present). All staff responsible for the undertaking of transactions, storing of transactional data and financial reconciling are required to read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Governors on an annual basis, or when relevant, to include newly developed security standards into the policy and inform staff accordingly of any changes.

Information Security Policy

The Integrated Centre' handle sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy and to ensure compliance with various regulations.

The Integrated Centre is committed to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end the Integrated Centre is committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Those staff handling sensitive cardholder data should ensure:

- They handle Integrated Centre and cardholder information in a manner that fits with their sensitivity.
- They protect sensitive cardholder information.
- They keep passwords and accounts secure.
- They always leave desks clear of sensitive cardholder data and lock computer screens when unattended.
- That any information security incidents must be reported, without delay, to the individual responsible for incident response which is the Integrated Centre Finance Manager.

We each have a responsibility for ensuring our organisation's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from the Integrated Centre Finance Manager.

Acceptable Use Policy

The Integrated Centre's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the organisation's established culture of openness, trust and integrity. The Integrated Centre is committed to protecting the employees, partners and the organisation from illegal or damaging actions by individuals, either knowingly or unknowingly.

- Staff should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Keep passwords secure and do not share their account details. Authorized users are responsible for the security of their passwords and accounts.
- All NNC workstations (and laptops where these may be used) should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Disciplinary Action

Violation of the standards, policies and procedures presented in this document by a member of staff may result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for not complying with the Policy.

Protect Stored Data

All sensitive cardholder data stored and handled by staff must be securely protected against unauthorised use, at all times. Any sensitive card data that is no longer required by the company for business reasons must be discarded in a secure and irrecoverable manner.

It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN Block under any circumstance

1. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level:

Official Sensitive Confidential data - Confidential data includes cardholder data. Any information relating to cardholder data, i.e., receipt books showing last 4 digits must be kept stored securely at all times.

Official Internal Use data – Use of information and data to be used in the financial reconciling of bank accounts at the direction of the Finance Manager.

2. Access to the sensitive cardholder data

All access to sensitive cardholder will be controlled and authorised.

- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to staff that have a legitimate need to view such information.
- No other employees should have access to this confidential data.
- Cardholder data is not to be shared with any 3rd party.
- The Integrated Centre will have a process in place to monitor the PCI DSS compliance status, responsibility for the overseeing of this process is delegated to the Finance Manager. Evidence of compliance will be displayed in public areas where any transactions may be taking place.

3. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Media is defined as any printed or handwritten paper, received faxes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner.
- Visitors must always be escorted by a member of staff when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all staff easily distinguish between other staff and Integrated Centre Users, visitors, and external contractors, especially in areas where cardholder data is accessible.
- All computers that store any sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

4. Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data etc.) must never be sent over the internet via email, instant chat or any other end user technologies.
- The transportation of media containing sensitive cardholder data to another offsite location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new secure location.

5. Disposal of Stored Data

- All data must be securely disposed of when no longer required by the organisation, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data whilst **on-site**, when no longer required, the required HMRC time period for all financial matters is 7 years from date of production.
- All hard copies of cardholder data must be manually destroyed **on-site** after the required period. An annual process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner. All hardcopy materials are shredded, incinerated or pulped so they cannot be reconstructed.
- The Integrated Centre' will have documented procedures for the destruction of electronic media. These will require:
 - All cardholder data on electronic media must be rendered unrecoverable when deleted e.g., through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
 - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked "To Be Shredded" - access to these containers must be restricted.

6. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A)
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the company.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Company security policies must be reviewed annually and updated as needed.

Security Management / Incident Response Plan

Employees of the company will be expected to report to the Finance Manager for any security related issues. The Finance Manager will effectively communicate all security policies and procedures to employees within the company and contractors.

In addition to this, the Finance Manager will oversee the scheduling of any updated system security training sessions, monitor the security policy outlined in both this document and at the training sessions and finally, oversee the incident response plan in the event of a sensitive data compromise .

Incident Response Plan

1. In the event of a suspected security breach, alert the Finance Manager, your line manager or a delegated manager, immediately.
2. The Finance Manager, or delegated manager, will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the Finance Manager, or delegated manager, will alert and begin informing all relevant parties that may be affected by the compromise.

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit:

http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html.

7. Vulnerability Management Policy

As part of the PCI-DSS Compliance requirements, the Integrated Centre will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

Network Security

- The Integrated Centre's systems are supported and run by the Local Authority who have the responsibility for providing a secure system network.
- As part of the PCI DSS compliance requirements a full system check with the Local Authority has taken place.
- Where any transactions may be taking place on portable electronic equipment the Integrated Centre's own Wi-Fi system will need to be regularly reviewed (cross-check with Online Safety Policy). The firewall rules will be reviewed by Pen Green Systems Administrator on a six month basis to ensure validity.
- A separate network segment must be implemented for wireless devices and users, where they are authenticated and firewalled as if they were coming from the Internet.
- Email with attachments coming from suspicious or unknown sources should not be opened. All such emails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any email which they suspect may contain virus.
- All removable media should be scanned for viruses before being used.

- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements and for a minimum of 90 days online and 1 year offline.

8. Password Policy

All staff with access to Integrated Centre's electronic financial systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- **Network access/passwords**

Users will be allocated appropriate access to systems controlled via User IDs and passwords. It is important to note that passwords must not be shared or written down by employees under any circumstances.

The system enforces the use of strong passwords, which contain at least six characters and are a mixture of alphabetical characters, numeric characters and lower and upper case for example: 7ove@pplEs **NB. This example must not be used.**

Appendix A – Agreement to Comply Form – Agreement to Comply With Information Security Policies

Employee Name (printed)

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to the company by third parties such as customers, will not be disclosed to unauthorised persons.. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Finance Manager, who is the designated information owner.

I have read and understand this policy, and I understand how it impacts on my . As a condition of continued employment, I agree to abide by the policies and other requirements found in the company security policy. I understand that failure to follow and undertake the guidance within this policy will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

Employee Signature