8
Confidentiality Policy

The Athelstan Nursery works closely with staff, committee, children and their families and recognise that this brings us into contact with confidential information.
Under no circumstances should any information be shared or discussed outside the nursery setting, except in the case of Safeguarding.

To ensure those working with or associated within the nursery in any way can do so in confidence we adopt the following procedures.

- All parents/carers can see details kept about their child and themselves at any time.
- All staff, committee members and Management Committee can see details kept about themselves at any time.
- Parents/carers will not be given access to the information kept on other children, members of staff, committee members or Management committee.
- Feedback given to parents/carers on their child's progress will be given directly to the parents/carers, unless they state a third party can be involved e.g. childminder/nanny.
- Information about a child's medical needs or status i.e. HIV or concerns about Safeguarding issues will be kept in a separate file and will only be available to authorised personnel and the Nursery Manager.
- Staff, Management committee, committee members, students and visitors to The Athelstan Nursery will be made aware of the importance of the confidentiality of information.
- Information about individual members of staff will not be given out to anyone without the permission of that person except in case of safeguarding.
- Data protection regulations and Freedom of Information Act requirements will be followed and explained to parents/carers during the settling in period.
- All confidential information will be stored securely.

The use of tablets by staff are strictly for the purpose of up- dating learning journals and are not permitted for personal use.

Data in Transit

Sensitive and confidential data must be treated with appropriate security by all who handle them. 'Appropriate' is not defined in terms of hard and fast rules, but is meant to be a degree of precaution and security proportionate to the potential impact of accidental disclosure. It is not possible to set out precautions and actions to cope with all circumstances and conditions, therefore staff handling sensitive and confidential data MUST assume personal responsibility and make considered

judgements in terms of how they handle data and if in any doubt seek support from their line manager.

Overall impact is determined by the degree of sensitivity of the data and the quantity involved, but we must remember that a single record about an individual can have a potentially massive impact on that individual if accidentally disclosed to others.

This policy is intended to prevent unauthorised disclosure of information by laying down clear standards of practice to maintain good security when using and taking sensitive or confidential data outside of their normally secure location.

This includes data in all formats – non-electronic (paper) and electronic (e.g. on PCs, tablets, laptops and removable storage media – i.e. USB memory sticks, PDAs etc.).

There are some 'common sense' precautions that you can take before taking or sending sensitive or confidential data outside of their normally secure location, these are:

- Check that you are not sending/taking more detail than is necessary i.e. will the information still meet the need if you remove the sensitive material or aggregate the data?
- Check that the data you are sending/taking are correct and appropriate.
- Check that you are sending the data to the correct person/address.
- Check how you intend to keep it secure.
- Staff to sign any equipment in an out when taking off site this includes paperwork and electronic tablets.
- All staff to have read and signed use of tablets policy.

If you are taking sensitive or confidential information with you in non-electronic (paper) records you must:

- Make sure that there is no other option available to you
- Never take the only copy with you if it is practical to make and retain a duplicate.
- You must assess the impact of loss of the original and make a copy if that impact is unacceptable
- Take only as much as necessary and only for as long as necessary
- Transfer it back to its normally secure location as soon as possible
- Take all reasonable precautions to keep the records safe and secure e.g.:
- Keep them with you whenever possible; lock them away securely when you can't
- Use a suitable container that prevents accidental loss and/or viewing by others
- Never leave them in plain sight in public places
- Report loss/theft immediately

Reporting lost data

In the first instance staff should report a loss of sensitive and/or confidential data to their manager. The manager will always report the loss to the management committee, detailing the circumstances of the loss and the nature of the data lost.

The management committee will determine the significance of the loss and will take appropriate action.

The management committee will investigate the circumstances of the loss and will be responsible for taking corrective action to prevent re-occurrence.

Nursery Manager: _____ Trustee: _____

Policy Date: _____ Review Date: _____