

**Duncan Private Hire**  
**Information & IT Security Policy**

**1. Policy Overview**

Duncan Private Hire is committed to protecting all information relating to children, families, staff, and Local Authority contracts.

Information security is a key part of safeguarding, and all employees involved in Home to School transport must ensure that personal and sensitive information is handled lawfully, securely, and responsibly at all times.

**2. Scope**

This policy applies to:

- All employees, drivers, escorts, contractors, and volunteers
- Anyone with access to Home to School transport information
- All devices and systems used for work purposes, including:
  - Mobile phones
  - Tablets
  - Laptops
  - Paper records

**3. Safeguarding & Data Protection Principles**

All Home to School information must be protected to ensure:

- Confidentiality – Information about children and families is only shared with authorised persons
- Integrity – Information is accurate and not altered improperly
- Availability – Information is accessible when required to keep children safe

Safeguarding information must always be treated as highly confidential.

**4. Roles & Responsibilities**

Management Responsibilities

Managers are responsible for:

- Ensuring staff only have access to information needed for their role
- Removing access promptly when roles change or staff leave
- Providing safeguarding and data protection training
- Reporting any data breaches to the Local Authority where required

Staff Responsibilities (Drivers, Escorts, Office Staff)

All staff must:

- Use information only for Home to School duties
- Keep personal and pupil information secure at all times
- Never share passwords or login details
- Lock vehicles, devices, and paperwork when unattended
- Report any loss, breach, or concern immediately

## **5. Handling Child & Family Information**

Information such as:

- Pupil names and addresses
- Routes and schedules
- Medical or behavioural information
- Safeguarding notes

must:

- Be shared only with authorised staff
- Never be discussed in public places
- Never be left visible in vehicles or public areas

## **6. Use of IT Systems & Mobile Devices**

- Only approved devices and systems may be used for work
- Mobile phones and tablets must be protected with passwords or PINs
- Work information must not be stored on personal devices unless authorised
- Devices must not be left unattended in vehicles

## **7. Remote & Mobile Working**

- Access to Home to School data is permitted only through approved systems
- Staff must ensure screens and paperwork cannot be seen by unauthorised persons
- Any lost or stolen device must be reported immediately

## **8. Printing, Paper Records & Disposal**

- Paper records should be kept to a minimum
- Documents must be stored securely when not in use
- Paper containing pupil or staff information must be shredded or securely disposed of
- Information should not be taken home unless authorised

## **9. Data Breaches & Incidents**

A data breach includes:

- Loss of paperwork
- Lost or stolen phone or tablet
- Sending information to the wrong person
- Unauthorised access to records

All breaches or suspected breaches must be reported immediately to management.

## **10. Compliance & Disciplinary Action**

Failure to follow this policy may:

- Place children at risk
- Breach Local Authority contracts
- Result in disciplinary action, up to and including dismissal
- Require reporting to the Local Authority or other bodies

## **11. Review**

This policy will be reviewed regularly to ensure:

- Compliance with Home to School Transport requirements
- Ongoing safeguarding effectiveness
- Alignment with data protection legislation

### **Key Message for Home to School Staff**

If information relates to a child, treat it as confidential, protect it at all times, and report concerns immediately.