

CLEARSPACE LEARNING LTD

DATA PROTECTION & PRIVACY POLICY

Company Registration:	15950890
Policy Owner:	Stuart Knox (Director)
Version:	1.1
Date of Issue:	September 2026 · Last Updated: October 2026
Review Date:	October 2027
Approved by:	Stuart Knox, Director

1. POLICY STATEMENT

Clearspace Learning is committed to protecting the privacy and security of personal information. We handle personal data in accordance with data protection law and hold ourselves to high standards of information governance.

This policy explains how we collect, use, store, and protect personal data relating to students, families, and other individuals who interact with our services.

Our Commitment:

- Process personal data lawfully, fairly, and transparently
- Collect data only for specified, legitimate purposes
- Keep data accurate and up to date
- Retain data only as long as necessary
- Keep data secure
- Respect individuals' rights over their data

2. LEGAL FRAMEWORK

This policy complies with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations 2003
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Children Act 1989/2004 (information sharing for safeguarding)
- Education Act 1996
- Freedom of Information Act 2000 (if applicable)

ICO Registration: Clearspace Learning is registered with the Information Commissioner's Office (ICO) as a data controller. Registration number ZB929305 (registered 3 July 2025; renewed annually).

3. ROLES AND RESPONSIBILITIES

3.1 Data Controller

Clearspace Learning Ltd is the data controller for personal information we process.
Registered Office: 40 The Bourne, Hook Norton, Oxfordshire OX15 5PB
Contact: info@clearspacelearning.com / 07986 622049

3.2 Data Protection Officer (DPO)

DPO: Stuart Knox
Contact: info@clearspacelearning.com / 07986 622049

The DPO is responsible for:

- Ensuring compliance with data protection legislation
- Advising on data protection impact assessments
- Monitoring policies and procedures
- Acting as point of contact with the ICO
- Responding to data subject access requests
- Training staff on data protection

3.3 Staff Responsibilities (Stuart Knox)

All staff must:

- Follow this policy and data protection procedures
- Keep personal data secure
- Only access data necessary for their role
- Report data breaches immediately
- Respect confidentiality
- Complete data protection training

4. DATA PROTECTION PRINCIPLES

We process personal data in accordance with six key principles:

4.1 Lawfulness, Fairness, and Transparency

We will:

- Have a lawful basis for all data processing
- Be open about how we use personal data
- Provide privacy notices to individuals
- Not process data in misleading or hidden ways

4.2 Purpose Limitation

We will:

- Collect data only for specific, legitimate purposes
- Not use data for purposes incompatible with those originally stated
- Clearly explain why we need data

4.3 Data Minimisation

We will:

- Only collect data we actually need
- Not collect "just in case" data
- Review data regularly and delete what's unnecessary
- Avoid duplication

4.4 Accuracy

We will:

- Take reasonable steps to ensure data is accurate
- Update or correct data when notified of inaccuracies
- Enable families to check and update their information
- Remove inaccurate data

4.5 Storage Limitation

We will:

- Not keep data longer than necessary
- Have clear retention schedules
- Review and delete data when no longer needed
- Anonymise data where appropriate for longer retention

4.6 Integrity and Confidentiality (Security)

We will:

- Keep data secure using appropriate technical and organisational measures
- Protect against unauthorised access, loss, or damage
- Train staff on data security
- Have procedures to detect and respond to breaches

5. LAWFUL BASIS FOR PROCESSING

We process personal data under the following lawful bases:

5.1 Contract

Processing is necessary to fulfil our contract with schools/local authorities to provide educational services.

Examples: Recording attendance, tracking progress, providing educational activities

5.2 Legal Obligation

Processing is necessary to comply with legal requirements.

Examples: Safeguarding reporting, health and safety records, employment law compliance (if staff employed)

5.3 Vital Interests

Processing is necessary to protect someone's life.

Examples: Medical emergencies, safeguarding situations requiring immediate action

5.4 Public Task

Processing is necessary to perform a task in the public interest (education).

Examples: Delivering alternative education provision, supporting children with SEND

5.5 Legitimate Interests

Processing is necessary for our legitimate interests (or third parties'), except where overridden by data subject rights.

Examples: Improvement of services, administrative purposes, business development

For children, we are particularly cautious and typically rely on other bases.

5.6 Consent

Where we rely on consent, it must be freely given, specific, informed, and unambiguous.

Examples: Photographs for promotional purposes, optional evaluations/research, non-essential communications

Consent can be withdrawn at any time.

6. SPECIAL CATEGORY DATA

Special category data (sensitive personal data) includes:

- Race or ethnicity
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sex life or sexual orientation

We process special category data about students under:

- Explicit consent of the parent or carer, or of the young person where they are able to give it (Article 9(2)(a) UK GDPR)
- Substantial public interest in safeguarding children and individuals at risk (Article 9(2)(g) UK GDPR and Schedule 1, paragraph 18 of the Data Protection Act 2018)
- Vital interests in emergencies

We need special category data to:

- Meet students' special educational needs and disabilities
- Provide appropriate support and adjustments
- Ensure health and safety
- Fulfil safeguarding duties

Extra safeguards apply:

- Data minimisation strictly applied
- Enhanced security measures
- Access restricted to those who need to know
- Privacy impact assessments conducted

Our appropriate policy document for this data is in Appendix A at the end of this policy.

7. DATA WE COLLECT

7.1 Student Data

We collect and process:**Personal Identifiers:**

- Name, date of birth, gender
- Address, postcode
- NHS number (if provided)
- Unique pupil number (UPN) if applicable

Contact Information:

- Parent/carers names and contact details
- Emergency contact information

Educational Data:

- Current school/educational setting
- Year group, Key Stage
- Attendance and punctuality records
- Academic progress and attainment
- Curriculum activities and engagement
- SEND information (diagnoses, EHCPs, support plans)
- Behavioural information and incident records
- Educational outcomes and destinations

Health and Wellbeing:

- Medical conditions, allergies, medications
- Dietary requirements
- Mental health information (where relevant to support)
- Safeguarding information (where necessary)

Referral and Commissioning:

- Reason for referral
- Referring school/professional
- Commissioning local authority
- Funding arrangements
- Previous educational placements

Photographs/Video:

- Images for educational purposes (with consent)
- Video for review/assessment (with consent)

7.2 Family Data

We collect:

- Parent/carer names and contact details
- Relationship to student
- Communication preferences
- Emergency contact information

7.3 Other Individuals

We may collect data about:

- Referring professionals (names, roles, contact details)
- Visitors (names, organisation, purpose of visit for safeguarding)
- Contractors (as required for safeguarding checks)

8. HOW WE COLLECT DATA

Data is collected from:

- Families (referral forms, intake meetings, ongoing communication)
- Referring schools and professionals
- Local authorities
- The student (observations, assessments, work produced)
- Other professionals (educational psychologists, social workers, health professionals)

We only request data we need and explain why we need it.

9. HOW WE USE DATA

We use personal data to:

Deliver Educational Services:

- Plan and deliver appropriate learning activities
- Track progress and development
- Assess needs and outcomes
- Provide feedback to students and families
- Support transitions and reintegration

Ensure Safety and Wellbeing:

- Fulfil safeguarding duties
- Manage health and medical needs
- Ensure health and safety
- Respond to emergencies

Communicate and Coordinate:

- Communicate with families about their child
- Liaise with referring schools and commissioning bodies
- Work with other professionals
- Provide reports and updates

Comply with Legal Obligations:

- Maintain attendance records
- Report safeguarding concerns
- Respond to subject access requests
- Meet contractual obligations to commissioners

Improve Our Service:

- Evaluate effectiveness
- Identify areas for development
- Monitor equality and inclusion
- Quality assurance

10. DATA SHARING

10.1 Who We Share Data With

We share personal data with:

Referring Schools:

- Progress reports
- Attendance information
- Behavioural incidents
- Safeguarding concerns

Commissioning Local Authorities:

- Contractual reporting
- Attendance and progress data
- Safeguarding information
- Invoicing details

Other Professionals (with appropriate consent/legal basis):

- Educational psychologists
- Social workers
- Health professionals
- SENCO/SEN teams

Emergency Services:

- In emergencies only (vital interests)

Regulatory Bodies:

- Ofsted (if applicable)
- Information Commissioner's Office (if required)
- Health and Safety Executive (RIDDOR reports)

Legal Obligations:

- Police (safeguarding, legal duty, or with warrant)
- Courts (court orders)

10.2 Information Sharing Principles

We only share information when:

- We have a lawful basis
- It is necessary and proportionate
- It is shared securely
- We record what was shared and why

We do not:

- Share data unnecessarily or routinely
- Share data without considering privacy implications
- Share special category data without extra safeguards

Families are informed about data sharing except where:

- Safeguarding concerns mean informing would increase risk
- Legal investigation would be prejudiced
- Legal obligation requires non-disclosure

11. DATA SECURITY

11.1 Technical Measures

We protect data through:

- Password protection on all devices
- Encryption of sensitive data
- Young people's records held on encrypted storage under Clearspace's control, not in cloud storage
- Antivirus and firewall protection
- Regular backups (encrypted and secure)
- Automatic screen locks on devices

- Secure deletion of data when no longer needed

11.2 Organisational Measures

We protect data through:

- Access controls – only those who need data can access it
- Confidentiality agreements (if staff employed)
- Clear desk/clear screen policies
- Secure filing – locked storage for paper records
- Shredding confidential waste
- Staff training on data protection
- Privacy by design – considering privacy in all new processes

11.3 Physical Security

- Office/storage: Locked premises at 40 The Bourne, Hook Norton
- Mobile working: Devices locked when unattended, not left in vehicles
- Paper records: Transported securely, stored in locked cabinets
- Disposal: Confidential shredding or secure digital deletion

11.4 Email and Communication Security

- Personal data is always sent by secure, encrypted email, or as a password-protected attachment with the password sent separately
- No personal or special category data is sent by unencrypted email
- Verification of recipient before sending
- Professional email used (not personal email for work purposes)

12. DATA RETENTION

12.1 Retention Schedule

Educational Records:

- Retained until the student's 25th birthday
- Or longer if serious safeguarding concerns

Safeguarding Records:

- Retained until the student's 25th birthday minimum
- Longer if serious case or ongoing concerns

Accident and Incident Records:

- 3 years minimum (adults)
- Until 25th birthday (children)

Routine Correspondence:

- Current academic year + 1 year

Financial Records:

- 6 years (legal requirement)

Contract and Commissioning Records:

- 6 years after contract ends

Recruitment and Vetting Records:

- Applicants who are not engaged: 6 months after the decision, unless they agree to us keeping their details
- Identity, qualification, reference, self-declaration and insurance records for associates and Governance and Advisory Panel members: 6 years after their engagement ends
- Right to work records: for the whole engagement plus 2 years
- Disclosure and Barring Service certificates: never copied or kept. We keep only the certificate number, level, issue date, date seen and the decision, on the Single Central Record, for 6 years after the engagement ends

- Records of allegations about adults working with children: 10 years from the date of the allegation, or until the person's normal retirement age if that is longer, reviewed regularly

12.2 Secure Deletion

When retention period expires:

- Digital data securely deleted (overwritten, not just deleted)
- Paper records confidentially shredded
- Backup copies also deleted
- Deletion logged

Archives: If data has historical value, it is anonymised before archiving.

13. INDIVIDUAL RIGHTS

Individuals have rights over their personal data:

13.1 Right to Be Informed

Fulfilled through:

- This policy
- Privacy notices provided at intake
- Clear communication about data use

13.2 Right of Access (Subject Access Request)

Individuals can request:

- Confirmation we hold their data
- Access to their personal data
- Information about how we use it

We will respond:

- Within one month
- Free of charge (unless manifestly unfounded/excessive)
- In accessible format

How to make a request:

- Contact Stuart Knox: info@clearspacelearning.com or 07986 622049
- Provide ID verification
- Specify what data you want

Note: For students' data, parents/carers can request on behalf of children. For older children, we consider the child's competence to make their own request.

13.3 Right to Rectification

Individuals can:

- Request correction of inaccurate data
- Request completion of incomplete data

We will:

- Respond within one month
- Correct or explain why we can't correct
- Notify third parties if data was shared

13.4 Right to Erasure ("Right to be Forgotten")

Individuals can request deletion when:

- Data no longer necessary for original purpose
- Consent is withdrawn (and no other lawful basis)
- Data processed unlawfully
- Legal obligation to erase

We may refuse if:

- Legal obligation to retain (e.g., safeguarding records)
- Public interest in retaining (e.g., serious case review)
- Legal claims need defending

13.5 Right to Restrict Processing

Individuals can request we stop using data (but not delete it) when:

- Accuracy is contested
- Processing is unlawful but they don't want deletion
- We no longer need it but they need it for legal claims

13.6 Right to Data Portability

Individuals can request:

- Their data in a structured, commonly used format
- Transfer to another provider

Applies when:

- Processing is based on consent or contract
- Processing is automated

13.7 Right to Object

Individuals can object to:

- Processing based on legitimate interests
- Direct marketing (we don't do this)
- Processing for research purposes

We will:

- Stop processing unless compelling legitimate grounds override
- Always stop direct marketing if requested

13.8 Rights Related to Automated Decision-Making

We do not use automated decision-making or profiling.

14. DATA BREACHES

14.1 What is a Data Breach?

A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data.

Examples:

- Lost or stolen device with personal data
- Email sent to wrong recipient
- Unauthorised access to systems
- Ransomware attack
- Loss of paper records

14.2 Reporting Data Breaches

All staff must:

- Report suspected breaches immediately to Stuart Knox
- Do not attempt to hide or minimise breaches
- Preserve evidence

Stuart Knox will:

- Assess the breach severity and risk
- Contain the breach
- Investigate what happened

- Report to the Information Commissioner's Office within 72 hours of becoming aware, unless the breach is unlikely to result in a risk to individuals
- Record every breach and near miss in the Data Breach and Near Miss Log, including those that are not reported
- Tell the council or commissioner where the contract requires it
- Notify affected individuals if high risk to their rights
- Document the breach and response
- Learn from the breach and improve security

15. PRIVACY NOTICES

Privacy notices are provided to:

- Families at intake (Student Privacy Notice)
- Referring schools and local authorities
- Other individuals whose data we process

Privacy notices explain:

- Who we are
- What data we collect
- Why we collect it
- Lawful basis for processing
- Who we share it with
- How long we keep it
- Individual rights
- How to complain

Privacy notices are:

- Written in clear, plain language
- Easily accessible
- Regularly reviewed and updated

16. CHILDREN'S DATA

Extra protections for children's data:

- We recognise children's data requires particular care
- Privacy notices are child-friendly where appropriate
- We consider the child's understanding and capacity
- We obtain parental consent where appropriate
- We do not process children's data for marketing
- Online safety is prioritised

Parental Responsibility:

- We verify who has parental responsibility
- We share data with those who have PR (unless safeguarding risk)
- We respect court orders regarding information sharing

17. CCTV AND RECORDING

CCTV:

- Clearspace Learning does not currently operate CCTV
- If introduced, privacy impact assessment would be conducted
- Signage would be displayed
- Retention and access strictly controlled

Audio/Video Recording:

- Sessions may be recorded for educational or safeguarding purposes
- Explicit consent obtained before recording
- Purpose explained clearly
- Recordings stored securely and deleted when no longer needed
- Not shared without consent (except safeguarding concerns)

18. PHOTOGRAPHY AND IMAGES

Consent is required for photographs or videos beyond routine educational documentation.

We will:

- Obtain explicit consent for promotional use
- Explain where images will be used (website, social media, publications)
- Allow withdrawal of consent at any time
- Never publish names alongside images online
- Store images securely
- Delete images when consent withdrawn or no longer needed

We will not:

- Share images on personal devices or accounts
- Use images for purposes not consented to
- Publish images that could identify vulnerable children (looked-after, safeguarding concerns)

19. THIRD-PARTY SERVICES

We use third-party services that process personal data:

Examples may include:

- Cloud storage, if used (not used for young people's records)
- Email services (e.g., Gmail, Outlook)
- Video conferencing (e.g., Zoom, Microsoft Teams)
- Finance/invoicing software

We ensure:

- Data processing agreements are in place
- Third parties meet GDPR standards
- Data is kept secure
- UK or EU-based servers used where possible
- We have the right to audit third parties

Families can request details of third parties processing their data.

20. USE OF ARTIFICIAL INTELLIGENCE

Clearspace Learning uses AI tools in two distinct contexts, each governed differently.

20.1 Back-Office Processing of Student Data

Where AI is used to help process student records (for example, drafting or reviewing EHCP-related material), Clearspace uses locally-run AI models (via Ollama/LM Studio) on a Clearspace-controlled device, rather than public or cloud-based AI services.

- Special category and EHCP data is not entered into public or consumer AI tools (e.g. ChatGPT, Gemini, Copilot) under any circumstances
- Local processing means data does not leave Clearspace's own device or get transmitted to a third-party processor, avoiding the data-sharing and international-transfer questions that cloud AI tools would raise
- AI-generated output is reviewed by Stuart Knox before use; AI assists drafting and analysis but does not make autonomous decisions about a student's education, support, or safeguarding
- This approach is kept under review as part of Clearspace's wider AI governance documentation

20.2 AI Used With or Around Students

Where AI tools are used with or around students (for example, in coding or STEM projects), this is governed by the Safeguarding & Child Protection Policy, which covers online safety and safeguarding considerations specific to that context.

20.3 Automated Decision-Making

As set out in Section 13.8, Clearspace does not use AI or any other tool to make automated decisions or profiling judgements about students without human review.

21. INTERNATIONAL TRANSFERS

We do not routinely transfer data outside the UK.

If international transfer is necessary:

- Only to countries with adequacy decisions or appropriate safeguards
- With explicit consent if required
- Documented and justified

22. TRAINING AND AWARENESS

Stuart Knox undertakes:

- Data protection training (completed and refreshed annually)
- Awareness of GDPR and DPA 2018 requirements
- ICO guidance and updates
- Sector-specific data protection guidance

If staff are employed:

- Induction includes data protection
- Annual refresher training
- Policy made available to all staff

23. COMPLAINTS

If individuals are unhappy with how we handle their data:

Step 1: Contact Stuart Knox (DPO)

- Email: info@clearspacelearning.com
- Phone: 07986 622049
- We will investigate and respond within one month

Step 2: If unresolved, complain to the ICO

- Information Commissioner's Office
- Website: www.ico.org.uk
- Helpline: 0303 123 1113
- Live chat available on website
- Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Individuals can complain to the ICO at any time without exhausting internal complaints first.

24. RELATED POLICIES

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct (confidentiality)
- Safer Recruitment Policy (Single Central Record)
- Privacy Policy
- Online Safety Policy
- Complaints Policy

25. POLICY REVIEW

This policy will be:

- Reviewed annually (September 2027)
- Updated in response to legislative changes, ICO guidance, or data breaches
- Made available to all data subjects

Who we are:

Clearspace Learning Ltd provides alternative educational provision for children and young people with SEND and additional needs.

Contact: Stuart Knox | 07986 622049 | info@clearspacelearning.com

What data we collect:

- Personal details (name, date of birth, address)
- Contact information
- Educational information (school, SEND, progress)
- Health information (medical conditions, allergies)
- Attendance and behaviour records

Why we collect it:

- To deliver appropriate educational support
- To keep your child safe
- To communicate with you and other professionals
- To meet legal requirements

Lawful basis:

- Contract with the commissioning school or local authority, and public task (providing education)
- Legal obligation (safeguarding, health and safety)
- Vital interests (emergencies)
- Consent (where appropriate)

Who we share it with:

- Your child's school
- The local authority commissioning the placement
- Other professionals supporting your child (with appropriate consent)
- Emergency services (if necessary)

How long we keep it:

- Until your child's 25th birthday (educational records)
- Longer if safeguarding concerns

Your rights:

- Access your data (subject access request)
- Correct inaccurate data
- Request deletion (in some circumstances)
- Object to processing (in some circumstances)

How to exercise your rights:

Contact Stuart Knox: info@clearspacelearning.com or 07986 622049

Complaints:

If unhappy, contact the Information Commissioner's Office: www.ico.org.uk or 0303 123 1113

POLICY APPROVAL

This policy has been approved by:

Stuart Knox

Director, Clearspace Learning Ltd

Date: September 2026

Next Review: October 2027

APPENDIX A: APPROPRIATE POLICY DOCUMENT – SPECIAL CATEGORY AND CRIMINAL OFFENCE DATA

This appendix is the appropriate policy document that the Data Protection Act 2018 (Schedule 1, Part 4) requires when we process special category data or criminal offence data to safeguard children and adults at risk. It forms part of this Data Protection Policy. Clearspace Learning Ltd is the data controller (Information Commissioner's Office registration number ZB929305). Stuart Knox, Director, is responsible for data protection.

A1. The data we process

- Health and disability information about young people. This includes diagnoses and needs (for example autism and ADHD), medical information (conditions, medication, allergies), Education, Health and Care Plans, and reports from occupational therapists, speech and language therapists and educational psychologists, where these are sent to us. What we receive varies from one young person to the next. It comes from parents and carers, young people, schools, the council and other professionals, and is used to provide safe, suitable education and to meet each young person's needs.
- Safeguarding records about young people and adults at risk, which may include health information and information about abuse or neglect.
- Criminal offence data about Stuart Knox, associates and Governance and Advisory Panel members: the Disclosure and Barring Service certificate number, level, issue date, date seen and the decision, and any self-declaration. The certificate itself is never copied or kept.
- We do not ask for or record ethnicity, religion, sexual orientation or similar information. If a family chooses to tell us something of this kind, we record it only where it is needed to meet the young person's needs or to safeguard them.

A2. Conditions for processing

- Health and disability information: explicit consent (Article 9(2)(a), UK General Data Protection Regulation). We ask for written consent at intake from the parent or carer, or from the young person where they are able to give it. This applies whether the information comes from the family or reaches us from a school, the council or another professional. Consent can be withdrawn at any time.
- Safeguarding records: substantial public interest, safeguarding of children and individuals at risk (Article 9(2)(g) and Schedule 1, paragraph 18 of the Data Protection Act 2018). We use this where we need to act to protect a young person from harm and where asking for consent would put them at risk or could not reasonably be done.
- Emergencies: vital interests (Article 9(2)(c)), for example giving medical information to paramedics.
- Accident, complaint and incident records: establishing, exercising or defending legal claims (Article 9(2)(f)).
- Criminal offence data: Article 10 and Schedule 1, paragraph 18 of the Data Protection Act 2018, applied to criminal offence data by paragraph 36. This is used only for safer recruitment checks on people who work, or may work, with children.

A3. How we comply with the data protection principles

- Accountability: Stuart Knox is responsible for data protection. We keep records of our processing activities and a log of data breaches and near misses, and we review this policy every year.
- Lawfulness, fairness and transparency: families and young people are told what we hold and why through the Privacy Policy and the student privacy notice, given at intake and in child-friendly form where appropriate.

- Purpose limitation: special category data is used only to deliver the commissioned provision, to keep young people safe, and to report to the commissioning school or council. It is never used for marketing and never sold.
- Data minimisation: we collect only what we need to teach and support the young person safely, and remove information that is no longer needed.
- Accuracy: we check key information with the family and the school at the start of a placement and at each review, and correct errors promptly.
- Storage limitation: records are kept only for the periods in Section 12 (Data Retention) and then securely deleted.
- Integrity and confidentiality: young people's records are held on encrypted storage under Clearspace's control, not in cloud storage. Personal data is sent only by secure, encrypted email or in password-protected files. Access is limited to Stuart Knox and, where he is covering or a concern is raised, the Deputy Designated Safeguarding Lead. Special category and Education, Health and Care Plan data is never entered into public or consumer artificial intelligence tools.

A4. Retention and erasure

The retention periods are set out in Section 12 (Data Retention). In summary: educational and safeguarding records are kept until the young person's 25th birthday, or longer where there are serious safeguarding concerns; accident and incident records are kept for at least 3 years for adults and until the 25th birthday for children; recruitment and vetting records are kept as set out in Section 12; and Disclosure and Barring Service certificates are never kept. When a period ends, digital data is securely deleted, paper is shredded and the deletion is logged.

A5. Review

This appendix is reviewed with the Data Protection Policy at least once a year, next in October 2027. It is kept for 6 months after we stop carrying out this processing, and is available to the Information Commissioner's Office on request.