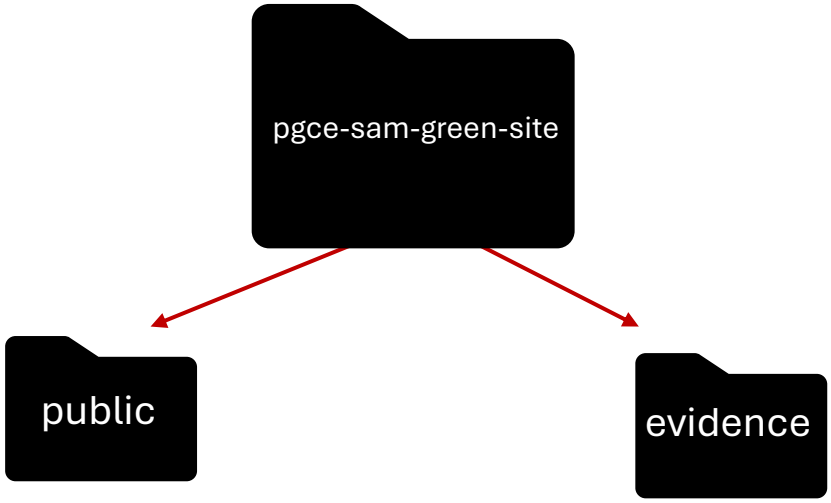
# Security Policy

*Last updated: 1st November 2025*



# Ten Safeguards in Plain English

1. **All content for this site lives in one secure folder.**
   Everything on this website is stored in a single, clearly defined location — a secure folder in Amazon Web Services called the **“pgce-sam-green-site” bucket**. This bucket is private by default.




1. **Site intrinsic files**
    - The HTML documents which describe the web pages themselves.
    - Various image files used to aid in navigation around the site (e.g. a briefcase icon to denote professional notes).

2. **Entries**

    Blogpost-style bodies of text describing how I have met the Teachers' Standards. Entries are the stuff of evidence.
    Where the evidence is to consist of private information, the entries will *refer* the reader to items in the evidence folder.

3. **Self-published works**
    - Some files will be in the public domain if they (1) contain no specific information related to individuals or specific schools and (2) are produced by myself.

      For example, a PDF file which is a graphic I designed, displaying the five areas of professional learning endorsed by Roehampton University.

1. **Documents I did not produce**

    Any documents for which I have no right to publish publicly on the Internet (e.g. a school's published behaviour policy).

2. **Documents I did produce**

    And have no **benefit** by being in the public domain, and potentially some risk.
    - All lesson Feedback Records (LFRs)
    - All lesson plans designed by the student teacher

The name of one folder, evidence, should not be taken as indication that it is the *only* place that evidence can be found. The name encourages the practice of keeping most information private by default.

2. **No sensitive pupil or personal data is stored here.**
   The teaching file contains lesson materials and professional reflections, but **no student names, photos, grades, or identifying details** appear anywhere in the bucket.

3. **The evidence files are private by design.**
   Even though the website itself is public, the evidence section is stored separately and cannot be accessed unless a visitor is issued a one-time activation link.

4. **Access is time-limited and personal.**
   Each assessor receives a unique link that works only once and only for a short period (typically 24 hours). After that, the link automatically expires.

5. **Every access request is checked automatically.**
   Amazon's global network (CloudFront) verifies that the browser holds a valid security token before allowing any evidence file to load.

6. **The site always uses secure connections.**
   Every page uses HTTPS encryption, so data travels safely between the browser and AWS. Modern browsers enforce this automatically.

7. **The site cannot be tricked by guessing addresses.**
   Knowing the web address of a private file isn't enough — CloudFront refuses to serve any evidence file without the correct signed authorisation.

8. **Access records and expiry times are monitored.**
   Each one-time link is recorded in a secure database with its creation and expiry time, allowing the owner to review or revoke access at any moment.

9. **Keys and passwords are stored securely.**
   The cryptographic keys used to sign access tokens are kept private and never appear on the website or in any public code.

10. **Public pages remain public; evidence remains private.**
    The rest of the site — information about the PGCE programme, teaching philosophy, and lesson plans — remains freely viewable to everyone.

# Technical Description

**Teaching File Security Policy**

**pgce.samgreencomputing.com**

The **Teaching File website** hosts professional evidence and reflections that form part of Sam Green's teacher training portfolio. While the site includes public pages that describe the training programme, lesson resources, and curriculum materials, certain areas—specifically the **evidence files**—are protected to ensure that only authorised assessors can view them.

This page explains how that protection works.

---

**1 · Principle of Least Privilege**

Only people who need to view evidence are granted access. The evidence materials are stored in a **private Amazon S3 bucket**; the bucket itself is not accessible over the public internet. Instead, all requests must pass through **Amazon CloudFront**, which acts as a secure content delivery layer.

CloudFront is configured so that it will not fetch or serve any evidence content unless the request carries a valid **cryptographic token**. Every other request is rejected at the network edge—before it even reaches the storage layer.

---

**2 · How Assessors Gain Access**

Each authorised assessor receives a **personal, one-time activation link**.
This link looks like:

https://pgce.samgreencomputing.com/activate?t=<unique-token>

The token in that link is a random, single-use value stored in a secure database (Amazon DynamoDB) with an expiry time. When the assessor clicks the link:

1. The request is routed to a small **activation service** (built with AWS Lambda and API Gateway).

2. The service checks that the token exists, has not been used before, and has not expired.
3. If valid, it issues three short-lived, signed cookies—each carrying a cryptographic signature produced by a private key held by Sam Green.
4. These cookies are automatically stored in the assessor's browser and are not accessible to JavaScript (HttpOnly and Secure attributes).
5. The assessor is then redirected to the /evidence section.

At this point, the original token is marked as "used" and can never be reused.
Forwarding the activation link to someone else simply results in an error.

---

**3 · How Access Is Enforced**

Whenever a browser tries to fetch an evidence file, CloudFront checks the signed cookies:

- Each cookie contains a **policy** stating *which paths may be accessed* (for example, https://pgce.samgreencomputing.com/evidence/*) and *until what time*.
- The policy is digitally signed using a private key known only to the site owner.
- CloudFront verifies the signature using a **public key** registered in its trusted key group.

If the cookies are valid and within their time window, CloudFront allows the request to proceed to S3.
If the cookies are missing, expired, or tampered with, CloudFront refuses the request.
No other service or script has the ability to bypass this check.

---

**4 · Additional Safeguards**

- **HTTPS enforced** across the entire domain; HSTS headers ensure browsers connect securely.
- **Strict content-security policies** prevent unauthorised scripts from running.
- **Minimal data retention**: tokens in the database expire automatically, and evidence cookies lapse after a short period (typically 24 hours).
- **Private key isolation**: signing keys are stored securely and never exposed on the website or to end users.

- **Audit simplicity**: every activation token and expiry time can be reviewed in DynamoDB, providing a clear access history.

---

**5 · Why This Is Secure**

Access to evidence relies on *cryptographic proof*, not on secrecy of web addresses. Only a browser that holds cookies signed by the correct private key—and issued via a valid, one-time activation link—can retrieve evidence files.
Even if someone knows the URL of a file, CloudFront will not serve it without that proof.

In short:

- **Private storage** ensures the content is never public.
- **One-time tokens** ensure links cannot be reused or shared.
- **Signed cookies** ensure CloudFront itself enforces access, not the browser.
- **Time limits** ensure access expires automatically.

These measures together guarantee that only designated assessors can view the evidence, and that their access is temporary, auditable, and cryptographically secured.