Gloucestershire Initial Teacher Education Partnership

ICT and Internet Usage Policy

Table of Contents

ICT AND INTERNET USAGE POLICY 3

Who is covered by this policy? 3

Relevant legislation and guidance 3

GITEP Staff 3

Trainees 4

- Professional Studies 4
- School Placements 4
- Use of phones and emails 4
- Remote working 5
- Digital images 5
- Personal devices and cloud storage 6
- Social Networking 6
- Teachers' Standards Part Two 7

Unacceptable use 7

Failure to comply with this policy 8

Links to other policies 9

Document history 9

ICT and Internet Usage Policy

Definition: GITEP staff refers to the Course Director, Course Administrator, Finance Manager, Lead Mentors and Subject Leads.

Who is covered by this policy?

- GITEP staff
- Trainees

Relevant legislation and guidance

- Data Protection Act 2018 The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2022
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools Education and Training (Welfare of Children) Act 2021
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people Meeting digital and technology standards in schools and colleges

GITEP Staff

GITEP staff are expected to adhere to the policies in place in their seconding schools. For those staff based at the Adfecto offices at Maisemore, they should adhere to any further requirements made by Adfecto policies.

Trainees

Professional Studies

Professional studies are held at partnership schools. Internet access is offered via guest networks.

School Placements

Whilst on school placement, trainees will have access to school networks and must adhere to school policies on acceptable use of IT.

To ensure trainees are aware, they will be required to read the school policy and sign to confirm they have read and understood the policy as part of their induction task.

Use of phones and emails

Partnership schools provide trainees with an email address. This email account must be used for work purposes only. All work-related business must be conducted using the email address the school has provided.

Trainees must not share their personal email addresses with parents and students and must not send any work-related materials using their personal email account.

Trainees must take care with the content of all email messages, as incorrect or improper statements can give rise to claims of discrimination, harassment, defamation, breach of confidentiality or breach of contract. Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Trainees must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information must be encrypted so that the information is only accessible by the intended recipient.

When sending emails to multiple recipients, the blind carbon copy (BCC) facility should be used to ensure email addresses are not visible to other recipients. This is especially important for external emails.

If trainees receive an email in error, the sender must be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If trainees send an email in error that contains the personal information of another person, they must inform the Professional Lead and Network Manager, or those

persons identified in the school policy immediately and follow the school's data breach procedure.

Trainees must not give their personal phone number(s) to parents or students.

Personal email accounts and phone numbers must not be used for school related work or to contact parents or pupils.

Remote working

Trainees may have access to a school's ICT facilities and materials remotely. When working remotely trainees must:

- Ensure only the minimum required information is taken off-site.
- Ensure access to any information cannot be seen by unauthorised people. This includes paper copies and computer screens.
- Never leave a device unattended and unlocked.
- Secure both ICT devices and paper documentation when not in use (e.g. Ensure in a bag, hidden from casual site).
- Trainees accessing a school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site.
- Trainees must be particularly vigilant if they use a school's ICT facilities outside the school and take such precautions as ensuring that security software is installed and working.
- When working remotely trainees must be careful that their facilities and materials are secure and cannot be overlooked to prevent any data breaches.
- Any breach or loss/theft must be reported immediately to the Professional Lead and the Network Manager, or those persons identified in the school policy.
- If ICT facilities must be used remotely, appropriate measures should be taken to prevent inadvertent data breaches (e.g. overlooking of the screen) by using devices like privacy filters and laptop locks.
- School ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with the GITEP data protection policy and those of our partnership schools.

Digital images

Trainees must not take photos of pupils or staff. Where pupil work is photographed, it should only be identified by initials.

Personal devices and cloud storage

School data should not be held on personal devices or personal cloud storage areas. Partnership schools will provide trainees with secure areas to hold school data during the course of their placements.

Where trainees are holding data from schools as part of their studies, they must adhere to the school's acceptable usage and data protection policies.

Social Networking

The key requirements are:

Trainees must check their privacy settings on social media platforms regularly. It is important that trainees recognise that their online activity can be seen by others so they should apply strong privacy settings and consider using a different name online.

Trainees have a responsibility to protect the reputation of the GITEP partnership, including themselves, their host school, staff and pupils.

Trainees must always treat fellow trainees, staff, colleagues, pupils and associates of the GITEP partnership with professionalism and respect whilst using social networking sites.

Social networking sites must be used responsibly, and users must ensure that neither their personal or professional reputation and/or the GITEP partnership's reputation are compromised by inappropriate postings.

Trainees must notify the GITEP Course Director and Headteacher of their placement school if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.

No GITEP partnership or partnership school information, communication, documents, videos and/or images must be posted on any personal social networking sites.

No details or opinions relating to any pupil are to be published on any website.

Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.

No opinions regarding another trainee or member of staff which could cause offence, can be posted.

No photos or videos, which show pupils of the school who are not directly related to the person posting them, can be uploaded to any site other than the school's website.

No comment, images or other material can be posted anywhere, by any method, that would bring the GITEP partnership or the profession into disrepute.

Users must not contact any pupil or parent/carer on any form of social media. If a student and/or parent/carer contacts you on social media, you must immediately notify the GITEP Course Leadership, Headteacher of your placement school and Designated Safeguarding Lead.

Users must also refrain from contacting or entering into correspondence with previous students and/or parents/carer of the partnership school in any form of social media, particularly where such contact could jeopardise the reputation of the GITEP partnership.

Users must not give pupils or parents/carers access to their social media sites e.g. being friends on Facebook. This also applies to previous pupils and their parents/ carers.

Teachers' Standards Part Two

Part Two of the Teachers' Standards requires teachers to demonstrate consistently high standards of personal and professional conduct. This includes teachers' online conduct. Trainees need to demonstrate they meet Part Two of the Teachers' Standards if they are to be recommended for Qualified Teacher Status at the end of their training year.

Unacceptable use

Unacceptable use of ICT facilities includes:

- Using ICT facilities to breach intellectual property rights or copyright
- Using ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the policies or procedures of any placement school
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages any member of the partnership, or risks bringing the partnership or partnership schools into disrepute

- Sharing confidential information about a partnership school, its students, or other members of the school community
- Sharing confidential information about GITEP staff, teaching staff or trainees
- Connecting any device to an ICT network in a partnership school without approval from authorised personnel
- Setting up any software, applications or web services on the network of a partnership school without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of that school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of a school's network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to a school's ICT facilities
- Causing intentional damage to a school's ICT facilities
- Removing, deleting or disposing of a school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, deleting, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to a member of the partnership
- Using websites or mechanisms to bypass a school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The partnership reserves the right to amend this list at any time and will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use.

Failure to comply with this policy

Any data breaches must be reported immediately to school staff – the Professional Lead, Data Manager and those persons identified in the school policy.

All breaches must be reported to GITEP course leadership. Where applicable, the DPO should be contacted in line with our Data Protection Policy; the Designated Safeguarding Lead should be contacted in line with our Safeguarding Policy.

Trainees who engage in any of the unacceptable activity listed above could be subject to disciplinary action. Depending upon the severity of the offence, a breach of this policy could be considered gross misconduct and expulsion from the course.

Any unauthorised use of partnership ICT systems, cloud-based ICT systems, the internet, email and/or social networking site accounts, which the GITEP Course Director or Headteacher of your placement school considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

Links to other policies

Safeguarding Policy
Data Protection Policy
Trainee Support Policy

Document history

Review Date	Significant Amendments	Made by	Approved by	Approval Date	Next review
Created: June 2023		KLF	Partnership Board		June 2026