Talbot House Preparatory School

Member of the Broadway Education Group

Acceptable Use (ICT) Policy

Aims

The Acceptable Use Policy sets out the boundaries of acceptable use of IT systems for staff and pupils, taking into account applicable data protection law (principally the UK GDPR and Data Protection Act 2018), applicable anti-radicalisation laws and best practice in safeguarding. The Acceptable Use Policy is a document that both staff and pupils are able to understand and sign up to, so it sets out key principles for day-to-day use of IT. The following information is for guidance and reflects the law and guidance as at the date it was published.

Applies to:

This policy applies to all members of the school community (staff or pupils) who use school IT systems, as a condition of access. Access to school systems is not intended to confer any status of employment on any contractors.

Available from:

This document is available to all interested parties from the School Office and on the School's website.

Monitoring and Review:

This procedure will be subject to continuous monitoring, refinement and audit by the Head teacher. The proprietors will undertake a formal review of this procedure for the purpose of monitoring the efficiency with which the related duties have been discharged, by no later than one year from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Adopted by: (signatures)	Date:
Head teacher: TWilson Mrs Tracey Wilson	January 2025

Talbot House Preparatory School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all pupils fulfil their potential.

Executive of the Board: Mrs J Broadway	January 2025
Review Date:	January 2026

Related Policies

There is a clear overlap in this area between staff and pupil conduct, data security, child protection, personal privacy online, and good practice including digital record keeping (including both email use and retention). This means that the Acceptable Use Policy does not stand on its own but must sit alongside related policies (applicable to staff or pupils), including where applicable:

(a) Privacy Notices (those aimed at pupils / parents and staff);

(b) Safeguarding Policy;

(c) Staff Code of Conduct;

(d) Data Protection Policy;

(e) Anti bullying Policy;

(f) Whistleblowing Policy;

(g) Online Safety Policy;

(h) Bring Your Own Device Policy'

(i) Use of Images of Children Policy;

(j) Data Breach Reporting Policy; and

(k) Retention of Records Policy.

The Acceptable Use Policy is not intended as a comprehensive Online Safety Policy. It is intended to be used in conjunction with the Online Safety Policy, which describes a more detailed framework for safe use of IT systems in schools (including monitoring).

Relevant background

This guidance continues to be updated and added to on an ongoing basis. Talbot House School consults the most up-to-date guidance from the organisations referred to below:

- The Department for Education (DfE)
- The Independent Schools Inspectorate (ISI)
- The Information Commissioner's Office (ICO)
- The Office for Standards in Education (OFSTED)

This policy and note is written having had regard to the following guidance and regulation:

- Keeping Children Safe in Education 2024 (September 2024)
- Working Together to Safeguard Children (December 2023)
- The Independent School Standards Regulations (April 2019)
- Prevent Duty Guidance for England and Wales (March 2024)
- DfE, Generative artificial intelligence (AI) in education – Policy Paper (October 2023)

- OFSTED, Ofsted's Approach to Artificial Intelligence (AI) – Policy Paper (April 2024)

Sharing and transfer of files and other data

When sending information digitally – whether to parents, local authorities, TRA or tribunal hearings, or Stage 3 complaints panels – consideration should be given to the appropriate level of security or encryption required, taking into account the nature and sensitivity of the data.

A non-digital solution may be preferable – especially if the security of the recipient's systems is unknown – but either way it is good practice to agree timing and methodology of delivery with the recipient, so as to ensure likely safe receipt and minimise the scope of complaint. Even registered post or guaranteed delivery carries uncertainties and can result in losses and delays. Couriers may be better, but not as reliable as personal delivery or collection. Talbot House School appoints an external IT provider for cloud storage and monitoring, and ensures that the contracts we hold with those providers have UK GDPR-appropriate data protection clauses, including as to data processing and any international transfers outside of the UK / EEA. The school undertakes due diligence with suppliers, who in turn must be prepared to provide adequate credentials on demand.

Email and digital retention

Talbot House School keeps and routinely deletes staff and school email records in a manner that ensures personal data is not kept for longer than is necessary, whilst ensuring policy safeguards are in place to minimise the risk of losing any critical records.

All emails are deleted after two years unless specifically filed for retention. Teaching and Leadership staff ensure that relevant information is being filed correctly using the school's cloud storage and management system.

Good practice in email use and record-keeping

Emails sent by school staff on school business are viewed as official records and regular training on acceptable use is provided at least every two years. The reputational, pastoral and career risks of over-using email – or using it casually and in unprofessional or intemperate language is emphasised to all staff, including governors and senior management. Equally, the benefits of keeping accurate, good quality contemporaneous records – objective, fair, and no longer or no shorter than they need to be are emphasised as, should they come to be needed in a staff disciplinary, parental complaint, subject access or litigation scenario, they will be important.

WhatsApp groups

Social media platforms such as WhatsApp can play a useful role in helping parents connect on a personal and private basis. However, there are several dangers that using these platforms can pose. Inappropriate or inaccurate content can be accidentally or purposefully shared. Comments which are defamatory, or distress other members of the school community can be widely distributed and difficult to remove.

Some platforms (such as WhatsApp) oblige users to share personal data to participate in a group. Some parents are not comfortable with this and hence will be excluded. The school does not therefore endorse the use of WhatsApp or other non-inclusive platforms for communication by the Parent Sub Committee, or by school-related groups set up by Classes or Year groups.

When discussing school-related topics on any form of social media, we advise parents to take note of some basic ground rules:

- Treat all members of the school community with kindness and respect
- Check all information with a reliable source or directly with the school before sharing with others
- Try to resolve any issues directly with the school before sharing problems with others
- Ensure you have the consent of other parents before sharing any of their personal data within the group, including contact details
- Under no circumstances share personal information about pupils or others at the school outside of the group or in any way which may be searched online

Online behaviour

As a member of the school community you should follow these principles in all of your online activities:

- The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the school's IT systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.

- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

Passwords

Passwords protect the school’s network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else’s computer or to confidential information to which you do not have access rights.

Use of Property

Any property belonging to the school should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the school bursar.

Use of school systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

Use of personal devices or accounts and working remotely

All official school business of staff and governors must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the Headteacher.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies, including [two-factor authentication, encryption etc.]

Monitoring and access

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, may be confiscated and examined if the school feels there is due cause. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

Tracking Devices and Technology

While the school is not responsible for individual settings on personal devices, [consistent with our policy on mobile device usage during school hours] our general position is that tracking technology that relies on location data sourced from third party devices should not be used on school premises or on school trips – given the potential privacy concerns for third parties. That said, the school is aware that there may be instances where such technology – whether, for example, for security of belongings or for parents' peace of mind as to children's whereabouts – can be used appropriately and proportionately. We would encourage parents and pupils to raise any such requests with us, for example in advance of a trip, so that we can discuss appropriate usage.

Compliance with related school policies

To the extent they are applicable to you; you will ensure that you comply with the school's Online Safety Policy, Retention of Records Policy, Safeguarding Policy, Anti-Bullying and Data Protection Policy,

Retention of digital data

Staff and pupils must be aware that all emails sent or received on school systems will be routinely deleted after 2 years and email accounts will be closed [and the contents deleted / archived] within 1 year of that person leaving the school.

Any information from email folders that is necessary for the school to keep for longer, including personal information (e.g. for a reason set out in the school privacy notice), should be held on the relevant personnel or pupil file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the Headteacher.

Breach reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and unsecure disposal.

The school must generally report personal data breaches to the ICO without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, they must report it immediately to a member of the senior leadership team, who will follow the Data Breach procedure.

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Breaches of this policy

A deliberate breach of this policy by staff or pupils will be dealt with as a disciplinary matter using the school's usual applicable procedures. In addition, a deliberate breach by any person may result in the school restricting that person's access to school IT systems.

If you become aware of a breach of this policy or the Online Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Headteacher. Reports will be treated in confidence wherever possible.

Acceptance of this policy

Please confirm that you understand and accept this policy by signing below and returning the signed copy to the school bursar.

I understand and accept this acceptable use policy (staff) :

Name: …………………………………………………………

Signature: …………………………………………………………

Date: …………………………………………………………

For younger pupils (below secondary school age)

Name of parent/guardian: …………………………………………………………

Signature: …………………………………………………………

Date: ………………………………………………………………..