Norfolk House School

Pupil IT Acceptable Use Policy

March 2026

Contents

Section Number	Section Title	Page Number
1	Aims	3
2	Scope and application	3
3	Regulatory framework	3
4	Publication and availability	4
5	Definitions	4
6	Responsibility statement and allocation of tasks	5
7	Physical safety	6
8	Acceptable interent useage	6
9	Email safety	8
10	Digital image safety	8
11	Avoidance of cyber-bullying	8
12	Use of mobile phones by pupils	9
13	Use of other personal communication devices by pupils	9
14	Tracker devices	10
15	Sharing nudes and semi-nudes	10
16	Inadvertently accessing inappropriate material	10
17	Risk assessment	10
18	Record keeping	11
19	Version control	11

1. Aims

1.1. This is the Pupil IT Acceptable Use Policy of Norfolk House School (**School**).

1.2. The aim of this policy is to ensure that technology is used safely and appropriately by all pupils, and monitored vigilantly by staff members in order for it to support and facilitate pupil learning.

2. Scope and application

2.1. This policy applies to the whole School including the Early Years Foundation Stage (**EYFS**).

3. Regulatory framework

3.1. This policy has been prepared to meet the School's responsibilities under:

3.1.1. Education (Independent School Standards) Regulations 2014;

3.1.2. Statutory framework for the Early Years Foundation Stage (DfE, September 2025);

3.1.3. Education and Skills Act 2008;

3.1.4. Children Act 1989;

3.1.5. Childcare Act 2006;

3.1.6. Data Protection Act 2018 and UK General Data Protection Regulation (UK **GDPR**); and

3.1.7. Equality Act 2010.

3.2. This policy has regard to the following guidance and advice:

3.2.1. Keeping children safe in education (DfE, September 2025) (**KCSIE**);

3.2.2. Preventing and tackling bullying (DfE, July 2017);

3.2.3. Sharing nudes and semi-nudes: advice for education settings working with children and young people (DCMS and UKCIS, updated March 2024);

3.2.4. Mobile Phones in Schools (DfE, updated February 2026)

3.2.5. Revised Prevent duty guidance for England and Wales (Home Office, updated March 2024);

3.2.6. Channel duty guidance: protecting vulnerable people from being drawn into terrorism (Home Office, updated December 2023);

3.2.7. Searching, screening and confiscation in schools (DfE, July 2022);

3.2.8. Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February 2019);

3.2.9. Relationships Education, Relationships and Sex Education (**RSE**) and Health Education guidance (DfE, July 2025);

3.2.10. Teaching online safety in schools (DfE, updated January 2023); and

3.2.11. Harmful online challenges and online hoaxes (DfE, February 2021).

3.3. The following School policies, procedures and resource materials are relevant to this policy:

3.3.1. Online Safety Policy;

3.3.2. Staff IT Acceptable Use Policy;

3.3.3. Social Media Policy;

3.3.4. Safeguarding and Child Protection Policy;

3.3.5. Anti Bullying Policy;

3.3.6. Risk Assessment Policy for Pupil Welfare;

3.3.7. Staff Code of Conduct;

3.3.8. Whistleblowing Policy;

3.3.9. Data Protection Policy;

3.3.10. Mobile Device and Camera Policy;

3.3.11. School Rules; and

3.3.12. Relationships Education Policy.

4. Publication and availability

4.1. This policy is published on the School website and in the Virtual Staffroom.

4.2. This policy is available in hard copy on request.

5. Definitions

5.1. Where the following words or phrases are used in this policy:

5.1.1. references to the **Proprietor** are references to the Board of Directors of Norfolk House School Limited.

5.2. In considering the scope of the School's acceptable use strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as technology).

6. Responsibility statement and allocation of tasks

6.1. The Proprietor has overall responsibility for all matters which are the subject of this policy.

6.2. The Proprietor is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of pupils. The adoption of this policy is part of the Proprietor's response to this duty.

6.3. To ensure the efficient discharge of its responsibilities under this policy, the Proprietor has allocated the following tasks:

Task	**Allocated to**	**When / frequency of review**
Keeping the policy up to date and compliant with the law and best practice	Head of Pastoral Care	As required, and at least termly
Monitoring the implementation of the policy (including the record of incidents involving the use of technology), relevant risk assessments and any action taken in response and evaluating effectiveness	" " "	As required, and at least termly
Seeking input from interested groups (such as pupils, staff, Parents) to consider improvements to the School's processes under the policy	" " "	As required, and at least annually
Formal annual review	Proprietor, Headmistress, Head of Pastoral Care	Annually

7. Physical safety

7.1. Pupils are taught about the dangers of electricity as part of the science and ICT programmes of study. They are advised how to behave appropriately when near electrical sockets and appliances and taught that they should not look directly at strong light sources such as the sun, lasers or projectors. Similarly, they are taught not to look directly into the light beam when working on the interactive whiteboards. Pupils are taught the correct posture for sitting at a computer and that sitting for too long can be unhealthy.

7.2. Pupils are taught the correct way to use ICT equipment as part of their programme of study and for Years 1 to 6. Pupils are advised that they should refrain from taking food and/or any liquids anywhere near the computers. Pupils are not allowed to access the ICT Suite in break times and tablets are held securely in a locked unit, overseen by the Head of ICT.

8. Acceptable internet usage

8.1. The School's Online Safety Policy sets out all the measures, including filtering and monitoring, which are taken to ensure that pupils and staff access the internet safely and securely, as well as the procedure to be followed in cases of misuse.

8.2. Members of staff in charge of pupils who have access to the internet must ensure that they are closely supervised at all times and that appropriate filters and control settings are in place.

8.3. Pupils have supervised access to laptop computers in the ICT Suite and tablets which are stored safely in a lockable unit and booked out by teaching staff as necessary. Before being permitted to use the school's laptops or tablets, pupils are instructed in their acceptable and responsible use. This instruction covers the purposes for which the devices may be used, the websites and applications that pupils may access, the requirement not to attempt to access inappropriate material or circumvent the school's filtering systems, and the importance of treating the devices with care.

8.4. Pupil are taught via the PSHCE and the ICT programme of study that the internet contains many websites which are not child-friendly and can be offensive and inappropriate to them. Pupils should make no attempt to access a website that they know to contain unsuitable material. Examples of such material include those websites which:

8.4.1. contains offensive language, images, games or other media;

8.4.2. is pornographic or indecent in any degree;

8.4.3. depicts scenes of explicit violence, degradation, humiliation or suffering;

8.4.4. is abusive;

8.4.5. encourages or supports the commission of a criminal offence;

8.4.6. is unlawfully discriminatory;

8.4.7. is intended or likely to harass or intimidate another person;

8.4.8. represents terrorist or extremist material.

8.5. Pupils must not use school equipment (laptop or tablet) to post, copy, share, forward or display material of the type referred to above.

8.6. Pupils must not:

8.6.1. access material which is inappropriate for their age;

8.6.2. access any social media websites, newsgroups or any website which allows them to interact with third parties;

8.6.3. should only access those websites which are related to their studies;

8.6.4. use the internet to access terrorist and extremist material

8.7. Pupils must:

8.7.1. report any filtering issues immediately to a member of staff.

8.8. Pupils are also taught that people who put their work on the internet may not want others to copy it, and they are advised to check that they have permission to copy work in line with copyright laws. Older pupils are taught about copyright, how to paraphrase, extract information or make it clear when something is quoted from another source, as well as how they should not present the work of others as their own.

8.9. Pupils accessing the internet at home are subject to the controls placed upon them by their parents. However, any home use of the internet made in connection with the school or school activities by any of its pupils will be subject to this policy and any breach dealt with as if the event took place in school. We expect all members of the school community to behave as positive ambassadors of the school in all school-related activities undertaken through the internet.

8.10. In order to teach its values and its dangers correctly, the school is mindful that its filtering and monitoring systems do not overly restrict pupils' ability to learn about its safe use.

9. Email safety

9.1. Some pupils will have their own email accounts at home. As these are independent of the school, they do not necessarily come with the safeguards that we set for email usage. Therefore, the school does not allow the use of personalised email accounts by pupils at school or at home for school purposes. Pupils are taught that using a personalised email account in school or for school use is not permitted.

9.2. Pupils are provided with a school email address which does not reveal their full name (eg joe.b@norfolkhousepupil.co.uk). They may only use the email address for two purposes:

9.2.1. to log into the School's online learning platforms; and

9.2.2. to learn how to use email under the direct supervision of a member of the School's teaching staff.

9.3. Pupils may not use the school email address at any other time or for any other purpose, and are instructed accordingly.

10. Digital image safety

10.1. The School takes digital photographs and video recordings of its pupils for a range of legitimate purposes including educational, pastoral and administrative (see the Pupil Privacy Notice published on the school's website). The School's Photography Policy contains details of the rules which govern the taking of photographs of children by staff.

10.2. The school seeks the consent of parents annually to take, store and use video recordings of pupils for further purposes which include promoting and publicising the school and its activities. Pupils will not be identified by full name in any publication without further consent being obtained.

10.3. Where the Headmistress gives her specific consent, pupils may take photographs as part of a particular learning experience. They must do so on cameras which are owned by the school (never personal cameras) and are not internet enabled, and always under the supervision of staff. Staff should adhere to the terms of the Photography Policy during such activity, and ensure that the pupils do likewise to the extent that they are applicable.

11. Avoidance of cyber-bullying

11.1. The School takes bullying very seriously and has robust procedures for identifying and dealing with it, as detailed in our Anti-Bullying Policy available on the school website or by request in hard copy. We expect all pupils to communicate with each other with respect and courtesy at all times. Pupils are

taught that cyber-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. Teaching is delivered through topics in PSHCE and ICT programmes of study on a regular basis throughout the school year and repeated as a spiral to develop awareness throughout their time at the school and build resilience for themselves and their peers.

11.2. As part of the above teaching programme, pupils are offered guidance on how to deal with aspects of bullying, including cyber-bullying, and are encouraged to speak to any member of staff in relation to any concerns. The Head of Pastoral Care will have responsibility for following up on bullying issues and noting any trends in incidents.

12. Use of mobile phones by pupils

12.1. Pupils are not allowed to have mobile phones in school. The DfE's guidance Mobile Phones in Schools is clear that all schools must be mobile phone-free environments by default.

12.2. In exceptional circumstances, permission should be sought from the Headmistress for a pupil to being a mobile phone into school. If so authorised, the pupil's mobile phone will be stored in the School Reception during the school day. During residential trips the use of mobile phones by pupils will not be allowed. Pupils may not use camera phones under any circumstances.

13. Use of other personal communication devices by pupils

13.1. Pupils are not permitted to bring personal communication devices onto the School's premises or on School trips or activities. For the purposes of this policy, a personal communication device means any device capable of sending or receiving messages, images, video or audio content, or accessing the internet, other than a mobile phone (which is addressed separately in section 12 above). This includes, but is not limited to, smartwatches, tablets, iPads, laptops, portable gaming devices with online or messaging functionality, and wireless earbuds or headphones with voice assistant capability. The School recognises that the boundary between a communication device and other technology is not always clear-cut; where there is doubt about whether a particular device falls within this prohibition, the decision of the Headmistress shall be final. Any personal communication device brought onto School premises in breach of this policy will be confiscated in accordance with the School's procedures for searching, screening and confiscation, and parents will be notified. Pupils may be permitted to bring a personal communication device on a residential trip where the Headmistress has given express prior written consent; any such permission will be subject to conditions set by the Headmistress.

14. Tracker devices

14.1. Pupils are not permitted to bring tracker devices, including GPS trackers, AirTags, smartwatches with location-sharing functionality, or any other device designed or used primarily to monitor or record the location of a person or object, onto the School's premises or on School trips or activities. This prohibition reflects the School's commitment to the privacy and wellbeing of all members of the School community, and the potential for such devices to be used covertly in ways that amount to surveillance or harassment. Any tracker device found in a pupil's possession will be confiscated in accordance with the School's procedures for searching, screening and confiscation. Concerns that a tracker device may have been used to monitor a pupil without their knowledge or consent will be treated as a safeguarding matter and dealt with in accordance with the School's Safeguarding and Child Protection Policy.

15. Sharing nudes and semi-nudes

15.1. Pupils are made aware of the risks of sharing nudes and semi-nudes (sometimes referred to as 'sexting') via the PSHCE and ICT programmes of learning. Pupils learn that creating, possessing or sharing nude or semi-nude images of anyone under 18 is illegal, even where all parties consent. Pupils are encouraged to apply safe and good practice outside school based upon their in-school learning. The School follows the guidance in *Sharing nudes and semi-nudes: advice for education settings working with children and young people* (UKCIS, updated March 2024). Any matters reported to the School in relation to the sharing of nudes and semi-nudes are followed up quickly and appropriately in accordance with the School's Safeguarding and Child Protection Policy.

16. Inadvertently accessing inappropriate material

16.1. In the event that inappropriate material is inadvertently accessed by a pupil, the pupil is taught to report this immediately to the member of staff supervising the session. The member of staff will then note the URL of the website in question, the time it was accessed, the name(s) of any pupil(s) who viewed the material, and which computer or device was being used. They will then follow up with the Head of ICT who will record it in a log and refer any incident to the Headmistress. This may result in the pupil not being allowed to access the internet until reassurances are given. The school reserves the right to monitor the websites visited on all computers owned by the school without forewarning.

17. Risk assessment

17.1. Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

17.2. The format of risk assessment may vary and may be included as part of the School's overall response to a welfare issue, including the use of individual pupil welfare (such as behaviour, healthcare and education plans, as appropriate). Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.

17.3. Headmistress has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

17.4. Day to day responsibility to carry out risk assessments under this policy will be delegated to Head of ICT who has been properly trained in, and tasked with, carrying out the particular assessment.

18. Record keeping

18.1. All records created in accordance with this policy are managed in accordance with the School's policies that apply to the retention and destruction of records.

18.2. All serious incidents involving the use of technology will be logged centrally in the technology incident log by the Head of ICT.

18.3. The information created in connection with this policy may contain personal data. The School's use of this personal data will be in accordance with data protection law. The School has published privacy notices on its website which explain how the School will use personal data.

19. Version control

Date of adoption of this policy	January 2020
Date of last review of this policy	5.3.26
Date for next review of this policy	5.3.27
Policy owner (SLT)	Head of Pastoral Care
Policy owner (Proprietor)	Chair of Directors