



Norfolk House School

Pupil IT Acceptable Use Policy

October 2021

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 internet useage | 6 |
| 9 | Email safety | 7 |
| 10 | Digital image safety | 8 |
| 11 | Avoidance of cyber-bullying | 8 |
| 12 | Use of mobile phones by pupils | 9 |
| 13 | Sexting | 9 |
| 14 | Use of hand-held devices by pupils | 9 |
| 15 | Inadvertently accessing inappropriate material | 9 |
| 16 | IT Acceptable Use Agreement | 10 |
| 17 | Risk assessment | 10 |
| 18 | Record keeping | 11 |
| 19 | Version control | 11 |
| Appendix 1 | IT Acceptable Use Agreement | 12 |

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, March 2017);
 - 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 2021) (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, December 2020);
 - 3.2.4. [Revised Prevent duty guidance for England and Wales](#) (Home Office, April 2021);
 - 3.2.5. [Channel duty guidance: protecting vulnerable people from being drawn into terrorism](#) (Home Office, February 2021);
 - 3.2.6. [Sexual violence and sexual harassment between children in schools and colleges](#) (DfE, May 2018);

- 3.2.7. [Searching, screening and confiscation: advice for schools](#) (DfE, January 2018);
 - 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, June 2019);
 - 3.2.10. [Teaching online safety in schools](#) (DfE, June 2019); 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 through the iPad Safe Use Agreement which they discuss in class. 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 iPads are held securely in a locked unit, overseen by the Head of ICT.

8. Acceptable internet useage

- 8.1. The School's Online Safety Policy sets out all the measures 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. Pupils 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:
 - 8.2.1. contains offensive language, images, games or other media;
 - 8.2.2. is pornographic or indecent in any degree;
 - 8.2.3. depicts scenes of explicit violence, degradation, humiliation or suffering;
 - 8.2.4. is abusive;
 - 8.2.5. encourages or supports the commission of a criminal offence;
 - 8.2.6. is unlawfully discriminatory;
 - 8.2.7. is intended or likely to harass or intimidate another person;
 - 8.2.8. represents terrorist or extremist material.
- 8.3. Pupils must not use school equipment (desktop or tablet) to post, copy, share, forward or display material of the type referred to above. Members of staff in charge of pupils who have access to the internet ensure that they are closely supervised at all times and appropriate filters and control settings are in place.
- 8.4. Pupils must not:

- 8.4.1. access material which is inappropriate for their age;
 - 8.4.2. access any social media websites, newsgroups or any website which allows them to interact with third parties;
 - 8.4.3. should only access those websites which are related to their studies;
 - 8.4.4. use the internet to access terrorist and extremist material
- 8.5. Pupils must:
- 8.5.1. report any filtering issues immediately to a member of staff.
- 8.6. 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.
- 8.7. 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.
- 8.8. 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 (g 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. In exceptional circumstances, permission should be sought from the Headmistress and, if authorised, the pupil's mobile device 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. Sexting

13.1. Pupils are made aware of the dangers of 'sexting' via the PSCHE and ICT programmes of learning and learn that the term relates to the writing and sharing of explicit messages and imagery with people they know or may not know. They are encouraged to use safe and good practice outside school, based upon their in-school learning. Any matters reported to the school in relation to sexting are followed up quickly and appropriately according to the school's Safeguarding Policy.

14. Use of hand-held devices by pupils

14.1. Pupils in Years 1 to 6 are allowed access to the school's set of iPads to enhance their learning and devices are stored safely in a lockable unit and booked out by teaching staff, as necessary. Safe Use Agreements (attached at the end of the policy) are discussed in detail in class with their teachers which pupils sign annually. These are also shared with parents so that all parties know the expectation of safe usage. Pupils are carefully supervised at all times when using iPads.

15. Inadvertently accessing inappropriate material

15.1. 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.

16. IT Acceptable Use Agreement

16.1. Children in Years 1 – 6 are required to read, discuss and sign an ICT acceptable use agreement on an annual basis which sets out the standards of conduct outlined above. A copy of the agreement is attached as Appendix 1.

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 | 21.6.21 |
| Date for next review of this policy | 21.6.22 |
| Policy owner (SLT) | Head of Pastoral Care |
| Policy owner (Proprietor) | Chair of Directors |

Technology acceptable use agreement for pupils

Norfolk House School understands the benefits technology can have on enhancing the curriculum and pupils' learning. However, we must ensure that pupils respect school property and use technology appropriately. To achieve this, we have created this acceptable use agreement which outlines our expectations of pupils when using technology, whether this is on personal or school devices and on or off the school premises.

Please read this document carefully and sign below to accept that you agree to the terms outlined.

1. Using technology in school

- 1.1. I will only use ICT systems, e.g. computers, laptops and tablets, which my teachers have given me permission to use.
- 1.2. I will only use the approved email account that has been provided to me by the school.
- 1.3. I will not store or use any personal data relating to a pupil or staff member for non-school related activities. If I have any queries about storing or using personal data, I will speak to my teachers.
- 1.4. I will delete any chain letters, spam, and other emails from unknown senders without opening them.
- 1.5. I will ensure that I get permission from my teachers before accessing learning materials, e.g. source documents, from unapproved sources.
- 1.6. During school hours, I will use the internet for school work only.
- 1.7. I will not share my passwords, e.g. to my school email account, with anyone.
- 1.8. I will not install any software onto school ICT systems unless instructed to do so by my teachers.
- 1.9. I will not use any removable media, e.g. encrypted USB drives on school devices.
- 1.10. I will adhere to the online safety guidelines I have been taught.
- 1.11. I will only use the school's ICT facilities to:
 - 1.11.1. Complete homework and coursework.
 - 1.11.2. Prepare for lessons and exams.
 - 1.11.3. Undertake revision and research.
 - 1.11.4. Gather or process information for extracurricular activities.
- 1.12. I will not use the school's ICT facilities to access, download, upload, send, receive, view or display any of the following:

- 1.12.1. Illegal material
- 1.12.2. Any content that could constitute a threat, bullying or harassment, or anything negative about other persons or the school
- 1.12.3. Anything offensive to others

2. Mobile devices

- 2.1. I will use school-owned mobile devices, e.g. laptops and tablets, for educational purposes only.
- 2.2. I will not use any mobile devices to take pictures of fellow pupils unless it is directed by the teacher.
- 2.3. I will not use any mobile devices to send inappropriate messages, images or recordings.
- 2.4. I will ensure that school-owned mobile devices do not contain any inappropriate or illegal content.
- 2.5. I will not take or store images or videos of staff members on any mobile device, regardless of whether or not it is school-owned.

3. Social media

- 3.1. I will not use any device to access personal social networking platforms.
- 3.2. I will not post or upload any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- 3.3. I will not post any material online that:
 - 3.3.1. Is offensive.
 - 3.3.2. Is private or sensitive.
 - 3.3.3. Infringes copyright laws.
 - 3.3.4. Damages the school's reputation.
 - 3.3.5. Is an image or video of any staff member, parent or pupil.

4. Reporting misuse

- 4.1. I will ensure that I report any misuse or breaches of this agreement by pupils or staff members to the Headmistress.
- 4.2. I understand that my use of the internet will be monitored by the school and recognise the consequences if I breach the terms of this agreement.
- 4.3. I understand that the Headmistress may decide to take disciplinary action against me in accordance with the school's Behaviour and Discipline Policy if I breach this agreement.

I acknowledge that I have read and understood this agreement, and ensure that I will abide by each principle.

| | |
|-------------------------------|--|
| Name of pupil: | |
| Signed: | |
| Date: | |
| Name of class teacher: | |
| Signed: | |
| Date: | |