



NORWICH SCHOOL

Pupil Digital Use and Safety Policy

This policy is reviewed by the Principal Deputy Head and Assistant Head (Quality of Teaching and Educational Development) annually. This policy was last reviewed and agreed on Trinity 2026. It is due for review in Trinity 2027.

Confirmed by:

Nicky Fairweather	Principal Deputy Head	Trinity 2026
-------------------	-----------------------	--------------

Version control

Version number	Date issued	Author / key contact	Change(s) summary
1.0	Trinity 2026	Alex Grant	New version

Contents page

Version control.....	1
Contents page	2
Introduction.....	3
Acceptable Use.....	3
Unacceptable Use.....	4
Filtering and Monitoring	4
Purpose and Scope	4
Filtering and Monitoring Systems	5
Operation, Safeguarding and Compliance	5
Roles, Responsibilities and Review.....	6
Artificial Intelligence (AI)	6
School iPads (1-1 devices).....	8
BYOD.....	12
Mobile Phone Guidance	12
Lower School.....	12
Blue Blazers (pupils in Lower 4–Upper 5 inclusive).....	13
Sixth Form.....	14
Exceptions.....	14
Working together	14
Principles of safe use.....	15
Password safety	15
Document control	17
Appendix 1: Summary for pupils issued with iPads.....	18

Introduction

Norwich School would like to support pupils in living well with technology – learning to be conscious, safe, proficient and responsible users of digital tools. The expectations set out in this policy apply to school owned, and personally owned devices - in so far as they affect the welfare of pupils or any member of the school community, or where the culture or reputation of the school might be compromised.

Acceptable Use

N.B. all KS3 pupils are reminded of this section of the policy in one of their first IT lessons of the academic year.

- Pupils are expected to use all school IT systems, devices, networks and online services safely, responsibly and primarily for educational purposes, whether using school equipment or personal devices, in or out of school, where their use is connected to Norwich School.
- Pupils must only access activities and content approved or permitted by a teacher or suitable adult, take proper care of all equipment, and seek help if unsure or if something goes wrong.
- Pupils must keep personal usernames and passwords secure and confidential.
- Pupils must behave online as they would expect others to behave towards them, showing respect in all communications and acting in a way that does not harm others or bring the school into disrepute, whether using school systems or not.
- Pupils must obtain permission before taking or sharing images of others and must protect personal information from being disclosed inappropriately.
- Pupils must respect copyright and intellectual property rights and take reasonable steps to check the accuracy and reliability of online information.
- Pupils may only use software, applications, online services, social media platforms and AI tools, including ChatGPT, where expressly authorised by a teacher or suitable adult and for approved educational purposes.
- Pupils must immediately report to a teacher or suitable adult any content, communication, behaviour or online activity that causes concern, distress, upset or presents a safeguarding risk.
- The school monitors use of its systems and registered personal devices to ensure safety and security. Continued use of school IT systems is conditional upon acceptance of this agreement.

Unacceptable Use

- Pupils must not access, create, download, store or share illegal, inappropriate, offensive, abusive, discriminatory, extremist or distressing material.
- Pupils must not misuse school systems, attempt to bypass filtering, monitoring or security controls, install unauthorised software, or make excessive downloads that may affect the performance or security of school systems.
- Pupils must not use school systems or networks for unauthorised gaming, gambling, shopping, file sharing, broadcasting, social media activity or use of AI tools without permission.
- Pupils must not use AI tools, including ChatGPT, to produce school-related work, submit work that is not their own, or gain academic advantage unless explicitly authorised by a teacher.
- Pupils must not send offensive, abusive, threatening or inappropriate messages, comments or images, engage in bullying or harassment, impersonate others, or act in any way that could harm another person or bring the school into disrepute, whether using school systems or personal devices.
- Pupils must not take, store, or share images, videos or recordings of others without permission.
- Pupils must not disclose personal, confidential or sensitive information about themselves or others without proper authority or consent.
- Pupils must not share usernames, passwords or other security credentials with any other person or attempt to access accounts belonging to others.
- Pupils must not deliberately access, search for or distribute material that is illegal, harmful, radicalising, sexually explicit or otherwise unsuitable for children.
- Pupils must not use school IT systems to engage in plagiarism, cheating, copyright infringement or any unlawful activity.
- Failure to follow this agreement may result in loss of access to IT systems, disciplinary sanctions, and, where necessary, involvement of external agencies or the police, including in cases of illegal activity or safeguarding concerns.

Filtering and Monitoring

Purpose and Scope

This policy outlines how the school uses internet filtering and network monitoring to maintain a safe, secure, and educationally focused digital environment. These

systems help protect pupils, staff, and the wider school community from inappropriate content, online threats, and misuse of school technology, while supporting the school's safeguarding responsibilities and compliance with statutory guidance on keeping children safe online.

This policy applies to all pupils, staff, volunteers, visitors, contractors, and any other users accessing the school network or school-owned devices, including wired and wireless networks, BYOD, school-managed devices, wearable technology, cloud services, and internet connections.

Filtering and Monitoring Systems

The school uses industry-standard filtering and monitoring systems to:

- Protect pupils from harmful or inappropriate online content
- Help prevent cyberbullying, radicalisation, online grooming, and other safeguarding risks
- Detect and discourage unsafe, unlawful, or harmful digital behaviour
- Protect school systems from malware, hacking attempts, phishing, and other cybersecurity threats
- Support teaching and learning through access to appropriate educational resources

Filtering systems may use:

- Website categorisation (e.g., adult content, gambling, violence, extremism)
- Real-time content analysis
- Safe search enforcement
- Automatic blocking of malicious domains

Monitoring systems may include:

- Keyword alerts linked to safeguarding concerns
- Behavioural analysis, including attempts to access blocked content
- Device and user activity logs
- Security alerts relating to malware or unauthorised access attempts

Filtering applies to all devices connected to the school network and, where appropriate, school-managed devices used off-site. Monitoring is proactive but proportionate and does not involve reading personal emails or documents unless there is a safeguarding or security concern and access is legally justified.

Operation, Safeguarding and Compliance

Filtering providers update blocklists continuously, and requests to blocked sites generate logs which may trigger alerts where patterns of misuse are identified. Staff may request access to educationally appropriate resources through an internal approval process.

Monitoring systems operate in the background and alert designated safeguarding or IT staff when concerning activity is detected. Alerts are risk-assessed and managed in line with safeguarding procedures, with serious incidents referred to senior leadership, safeguarding agencies, or law enforcement where required. All monitoring complies with data protection legislation, including the principles of necessity, proportionality, and minimisation.

Filtering and monitoring support the school in meeting obligations under:

- Keeping Children Safe in Education (KCSIE)
- Prevent Duty
- Data Protection Act and UK GDPR
- Health and Safety duties
- Acceptable Use and Online Safety policies

Roles, Responsibilities and Review

Senior Leadership Team

Must ensure filtering and monitoring arrangements meet statutory requirements and review policy effectiveness annually

Designated Safeguarding Lead (DSL)

Will receive and investigate safeguarding alerts and coordinate follow-up action where required

IT/Network Team

Will manage filtering and monitoring systems, review logs for security concerns and ensure systems remain updated

Staff

Will report concerns relating to student online behaviour and model positive digital citizenship

Students

Will use technology responsibly and follow the Acceptable Use Policy

This policy is reviewed annually, or sooner where significant changes occur in legislation, safeguarding guidance, or technology.

Artificial Intelligence (AI)

Norwich School is chiefly concerned with cultivating human intelligence. In so far as Artificial Intelligence (AI) can help with this objective, it can be used as an educational tool. The possibilities of AI are extensive, and its use can enhance the pupil experience in a meaningful way. Nevertheless, use of AI should always acknowledge the parameters set by the following guiding principles:

- 1. In the age of AI, the cultivation of human intelligence and creativity remains an intrinsic good.**
- 2. AI should be used to support learning, not undermine it. AI makes pupils' acquisition of knowledge more important, not less.**

3. Pupils and teachers must develop AI literacy. Understanding how to interact with AI thoughtfully, effectively and ethically is essential.

4. Relationships and communication between teachers, pupils and parents must not be diminished by AI.

5. AI use must always be safe, ethical and within the bounds permitted by regulation

'AI' is a broad umbrella term. In our context, the following guidance primarily relates to Large Language Models and Generative AI:

Examples of AI use to support learning:

- Pupils can be educated about AI and its uses as part of the curriculum where Heads of Department deem this to be relevant.
- Under the direction of a teacher (and if permitted by a Head of Department), AI can be used by pupils; they can be taught about it, as well as how to use it. This will often be in a context where AI is the explicit focus of the learning and use must adhere to age restrictions.
- Pupils should be encouraged to think critically about the material that AI produces. To 'prompt' effectively requires knowledge about the domain in question and an ability to write clearly. Knowledge is then required to sense-check the results that are produced.
- If approved by a Head of Department, pupils can use AI to help with their revision (producing revision materials, practice questions etc.) and to guide initial research queries. They should be guided in this by their teacher, ensuring that research prompts do not cross over into generating text or structures for submitted work.

Boundaries of AI use in learning:

Pupils are discouraged from using AI to bypass the acquisition of skills and knowledge that we want them to develop as learners. For example, if pupils use AI to plan or write an essay, or to give immediate answers to mathematical or scientific problems, they are not cognitively engaged and are damaging their learning.

- Pupils must adhere strictly to the age restrictions and terms of use of individual AI platforms. For most major platforms (including ChatGPT/OpenAI), pupils under the age of 18 are legally required to have explicit parental permission.
- Pupils should not use AI to access or create harmful or inappropriate content.
- Pupils should never use AI to produce work that they pass off as their own (see below).
- Pupils should not enter personal data, sensitive information or identifiable details about staff or pupils into an AI system as this information would then enter the public domain.
- Pupils should only ever use AI for academic work under the explicit guidance of their teacher and with the agreement of the Head of Department.

- If pupils do use AI for any part of their work, it must be referenced or acknowledged clearly. If teachers suspect the work is not the pupil's own, they may face consequences for plagiarism as set out in the Behaviour Support and Intervention Policy.
- As with any source, generative AI should not be seen uncritically as a source of reliable information. The content they produce can be inaccurate, biased, inappropriate, their sourcing can be unclear, and they can 'hallucinate'.
- AI should not be used for Non-Examined Assessment. Pupils who submit work for public examinations that is not their own will have committed malpractice, in accordance with JCQ regulations. This may attract severe penalties.

AI, academic integrity and authentication:

Where a teacher has doubts about the authenticity of work submitted (for example, a sudden shift in vocabulary, complexity, or writing style), the school relies on human judgment rather than automated detection software to investigate the matter. The teacher will investigate by holding a conversation with the pupil to check their understanding, comparing the submission to previous work, or asking the pupil to talk through their research path and explain their vocabulary choices. If a teacher is not satisfied that the work is the pupil's own independent output, the pupil will be asked to redo it under controlled, supervised conditions, and sanctions in the Behaviour Support and Intervention Policy may be applied.

Where pupils have questions or concerns about AI use, they should speak to a teacher, the Head of Computer Science, IT Support or the Assistant Head (Quality of Teaching and Educational Development).

School iPads (1-1 devices)

This section of the policy applies to pupils who have been issued with a school-managed iPad from September 2026.

1. Receiving and returning the device

1.1. Receiving the device

This policy applies from the moment the device, stylus, keyboard case and chargers are issued to the pupil. The device remains school property and all pupils issued with a device should adhere to this policy.

1.2. Returning the device

At the end of U5, or when the pupil leaves the school (whichever is sooner), the device, stylus, case and chargers must be returned to the school in good condition with only reasonable wear and tear.

2. Taking care of the device

2.1. General precautions

- The device should be kept in its case.
- The device should never be lent to another person.

- Screens should be protected; they can be damaged if subject to rough treatment or excessive pressure. Only a clean, soft cloth should be used to clean the screen. Pupils are permitted to attach a screen protector.
- Food and drink should be kept away from the device.
- Charging cables should be inserted and disconnected carefully to prevent damage.
- Devices should never be left unattended anywhere outside the school or pupil's home.

2.2. Device security

- Devices are protected by a passcode. Pupils are prohibited from sharing this passcode with anyone else except a member of staff or parents when requested.
- iPads should always be locked if unused or left unattended.

2.3. Storing devices around school

- Pupils should keep the device in their bag when they are moving around the school site.
- Bags should only be left in designated covered bag racks or lockers around the school site.
- Bags (containing devices) should never be left unattended in any other location. They should never be left exposed to rain, nor should they be left anywhere around the Close that can be accessed by members of the public.
- If a device is left unattended outside designated spaces, it should be taken to the IT support desk in the Palace.

3. Using the device at school

Devices are intended for use at school each day. It is part of the essential equipment list and is included in regular 'Ready to Learn' tutor checks. Pupils are responsible for bringing their device to lessons unless specifically instructed not to do so by their teacher.

3.1. Charging

- Pupils must bring their device, stylus and keyboard case to school fully charged each day. There are no opportunities to charge these during the school day.

3.2. Devices left at home

- If the device is left at home, or it has insufficient charge, pupils are responsible for getting the work completed as if they had the device present. Devices are unavailable for loan in this scenario.

3.3. During lessons

- Pupils should only get the device out of their bag if told to do so by the subject teacher. Devices should only be out when they are being used.
- The use of messaging, email, personal apps and recreational use is strictly prohibited during lessons.

- Unless instructed otherwise, pupils should lay the tablet flat on the desk so that the screen is not a barrier between them and the rest of the class.
- Ultimately, the use of devices in lessons is at the discretion of the individual teacher.

3.4. Outside of lessons

- Pupils should not use their device outside of lessons without teacher permission. Devices should not be used outside, in classrooms during break or lunch, in any corridors or communal areas, toilets or in the refectory.
- An exception is that devices can be used in the libraries during break, lunchtime or after school.

3.5. Digital Organisation

Pupils are responsible for ensuring that they organise their files. All work should be saved to OneDrive and not saved locally to the device. It is the pupil's responsibility to ensure that work is not lost due to the device malfunctioning or accidental deletion. Help and advice is available from members of the Computer Science Department and the IT Team.

3.6. Photographs/ images

- During the school day, the camera should only ever be used with permission from a teacher.
- Photography/ video of others – pupils or staff - is prohibited unless given explicit permission by a teacher. Images of other people may only be made with the permission of those in the photograph/ video.
- The camera must never be used to take inappropriate, illicit, or sexually explicit photographs or videos, nor should it be used to embarrass anyone in any way. Any use of the camera in toilets or changing rooms, regardless of intent, will be treated as a serious disciplinary matter.
- Posting of images or video taken using the device should never be posted on the internet into any public forum.

3.7. Sound/ music

- All sound and music must be muted (including notifications) unless permission is granted by a teacher for educational purposes.

3.8. Printing

- If directed by a teacher, pupils may print from the device in school. There are limits on the amount of printing pupils are able to do. If pupils have any difficulties, they should speak to IT Support.

4. Using the device outside school

4.1. Use at home

- Pupils are encouraged to use their device at home for their homework and to help their learning. This policy applies to use of the device outside of school.

- Note that Smoothwall filtering applies at home as well as in school; device use can be monitored by the IT Team.
- Devices will shut down at a set time in the evening to ensure that pupils are screen-free before going to sleep.

4.2. Use in public places

- Pupils are allowed to use their devices in public places. However, pupils should be circumspect about their use. Devices should never be left unattended in a public place.

5. Apps, content and updates

The apps and content installed by the school must not be removed. From time to time, the school may add further apps or programmes for use in teaching and learning. Updates, management of the devices and installation of new apps will be administered and installed centrally by the IT Department. Pupils are unable to remove apps or change settings.

6. Theft, damage or loss

If a device is stolen, damaged or lost, the following processes should be followed:

6.1. Theft

The IT department must be alerted as soon as possible to allow them to remotely lock and wipe the device rendering it unusable. A crime number must be obtained from the police and then shared with the IT Department who will in turn obtain a replacement device.

6.2. Damage

The pupil must report damage to the IT Department who will log it centrally. A loan device will be available for collection later that day and the damaged device will be repaired and returned at which point the loan device must be returned upon collection of the repaired device.

6.3. Loss

The pupil must report the device lost to the IT department who will attempt to track it via location services to narrow down its location. Pupils will not be given a loan device but will, instead, be asked to find the device. If the device is not found after one week, then a replacement device may need to be issued. The IT department will then lock and wipe the device remotely, rendering it unusable.

6.4. In cases of theft, damage or loss, a £50 excess and administration charge will be added to the pupil's fee bill. Lost styluses can be replaced by the IT department and the replacement cost will be added to the fee bill.

6.5. If theft, damage or loss is repeated or a consequence of deliberate, malicious or negligent behaviour, the school may pass on the full replacement cost to parents. The pupil may also face consequences detailed in the Behaviour Support and Intervention Policy.

7. Acceptable use and monitoring

- 7.1. The provisions set out in relation to acceptable and unacceptable use in the rest of the Pupil Digital Use and Safety Policy apply to the use of school iPads, both in and out of school.
- 7.2. Device use is monitored by the school's digital monitoring systems. This includes geo-location. Pupils should be aware that the Smoothwall internet filtering and monitoring system operates both on and off the school site.
- 7.3. Unacceptable use may result in confiscation of the device by a teacher, followed by sanctions as set out in the Behaviour Support and Intervention Policy.
- 7.4. If misuse is persistent, the school reserves the right to remove the device from the pupil.

BYOD

Pupils in M5, U5, L6 and U6 may bring personal devices, including laptops and tablets, into school to support their learning. Use of personal devices must always be appropriate, educational, and in line with acceptable use as set out in this policy.

Mobile phone restrictions during the school day continue to apply, particularly in shared spaces and during lessons unless permission has been given by staff.

Any personal device connected to the school network is subject to the school's monitoring and filtering systems. Pupils are responsible for the security and safe use of their own devices, including ensuring that passwords, updates, and appropriate security software are in place.

The school accepts no responsibility for loss, theft, damage, data loss or technical support relating to personal devices and reserves the right to withdraw BYOD access where misuse occurs.

Mobile Phone Guidance

We appreciate that many families are choosing to reconsider or delay the use of smartphones by their children and we are supportive of this. We would like to emphasise that pupils do not require a smartphone in school.

Lower School

- Where pupils walk or travel independently, they may bring a mobile phone to school.
- All phones must be handed in at reception and signed in, then collected at the end of the day, or when leaving.
- If a pupil is found in possession of or using a phone during the school day:
 - It will be confiscated

- o They will be asked to switch the phone off and confirm their name - it will be passed to one of the Deputy Heads
 - o An appropriate consequence will be issued.
- Confiscations are monitored; repeated infractions may result in disciplinary intervention and parents/guardians may be required to collect the phone.
- Pupils may wear a smartwatch if it is not connected to other devices.
- Smartwatches with cellular or Wi-Fi capability will be treated as mobile phones and subject to the same rules.

Blue Blazers (pupils in Lower 4–Upper 5 inclusive)

- The use of phones is always prohibited during the school day (on site, transport and off-site activity).
- A smartphone is not required for any educational purpose.
- Where a choice is made to bring a phone to school, we suggest a 'brick-phone' option.
- Any phone should be always secured in a bag or blazer pocket - from morning arrival in The Close until 16:00.
- Any phone should be switched off or on silent with no notifications.
- Where trips and visits extend beyond the school day, use is at the discretion of accompanying staff.
- Pupils should have a paper copy of their timetable with them daily; issued in September, pupils can request a new copy be printed at 71a Reception.
- The use of contactless payment with a phone is not allowed (pupils should have a debit card or cash to buy items at breakfast, breaktime or at charity events).
- Smartwatches and other wearable technology are not allowed.
- Any phone seen will be confiscated - the pupil will be asked to turn it off and confirm their name. It will be handed in at the Principal Deputy Head's office (in School House) and be stored securely.
- The phone can be collected at 16:00. Pupils may not use the front blue door of School House; they must enter the building by the door from the Quad and be polite in their interactions with staff.
- Confiscations are monitored and the following interventions applied:

Confiscation frequency	Intervention
1	Verbal warning
2	Friday after school detention
3	Phone secured until parent / carer collects. Meeting with parent and pupil to agree next steps

Sixth Form

- In alignment with DfE guidance, pupils in the Sixth Form are permitted to use their phone in certain locations, reflecting this period of education as one of increased independence and responsibility.
- Phones should be on silent during the school day.
- Sixth Form pupils are permitted to use their phones within Sixth Form areas or if studying in the Reynolds Library.
- Phones must not be used when moving around the site, or in shared spaces such as playgrounds, the Cathedral and Refectory.
- Phones may only be used during lessons with teacher permission.
- Pupils should not presume they can charge their phones during lessons; they must seek permission from a teacher.
- Headphones may only be used in Sixth Form spaces.
- If a phone is being used inappropriately, it will be confiscated as outlined above.

Exceptions

- If pupils need to contact home, they can ask to use a landline at Reception in 71a or a staff office.
- Pupils in U5 may use their phones when they have permission to be off-site, being mindful of personal safety.
- Reasonable adjustments may be made for a pupil with additional learning needs or medical requirements to use a mobile phone and headphones. In such cases, staff will be aware of parameters, and the phone should only be used as agreed.
- The use of phones in libraries after school is permitted to aid study.

Working together

- We respect the range of personal choices families make around technology. There is no expectation from the school for pupils to own a mobile phone.
- Through PPD lessons and pastoral input the school will encourage respectful, responsible and safe use of technology. We encourage families to maintain open dialogue at home regarding digital devices and personal use. The school subscribes to the Tooled Up Education platform where all parents / carers have access to a library of research-based resources.
- We ask that parents and guardians support the school's approach by refraining from contacting pupils during school hours. In urgent situations, parents should contact the school office directly.
- Staff are asked to be mindful of their own use of phones around site.
- Staff will be considerate to when pupils have access to Teams outside of the school day when sending messages, setting Assignments etc.

- Staff understand that they cannot expect pupils to respond to communications sent on the day, during the school day.
- We ask that pupils check their school email, Teams messages and Assignments (all homework is set this way) in the evenings.

Principles of safe use

- Pupils are reminded of the illegal nature of sending indecent images of themselves or others; such cases will be dealt with appropriately using safeguarding practice and procedure, including informing the authorities, if necessary.
- Pupils must ensure that material stored on their mobile phones does not contain violent, degrading, discriminatory or explicit content. The sharing of such material can be a criminal offence.
- Pupils are strongly encouraged not to communicate with individuals unless they are known to them.
- Pupils are advised to discuss social media use with their parents/carers considering age restrictions and privacy settings.

Password safety

N.B. all pupils in L4 receive a lesson on this topic in the Michaelmas Term.

Pupils have individual school network logins, email addresses, and storage folders on the server. Pupils are regularly reminded of the need for password security.

All pupils should:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed when required and at least annually
- not write passwords down
- not share passwords with other pupils or staff

A good password is one that is difficult for others to guess. Current best practice is to use a 'passphrase' made up of three random words, rather than a single word password. A good password is one that can be remembered easily and typed quickly so that anyone looking over your shoulder will not be able to see what you are typing.

A password must:

- be at least sixteen characters long
- contain at least one upper case and one lower-case letter
- not appear in any dictionary or any other list
- have no personal connection with the owner

A bad password is one that is easy for others to guess, or so difficult to remember that the owner writes it down. Malware that is designed to break passwords use lists of commonly known weak passwords, and so dictionary words are more likely to succeed when a password, as described above, is not used. A determined hacker will use social media profiles to gather personal information that staff may use in passwords.

Document control

Document title:	Pupil Digital Use and Safety Policy
Prepared by:	Alex Grant, Assistant Head (Quality of Teaching and Educational Development)
Authorised by:	Nicky Fairweather, Principal Deputy Head
Published location(s):	▪ Norwich School website ▪ The Hub
Other internal policies / documents referenced:	▪ Behaviour Support and Intervention Policy
External documents referenced:	▪

Appendix 1: Summary for pupils issued with iPads

1. Look after the device: keep your iPad, case, stylus and charger with you at all times and return them in good condition.
2. Stay secure: use a passcode to protect your iPad and never share it with anyone other than a teacher or your parents. Never lend your device to another person.
3. Keep it safe: keep your iPad inside your bag while moving around school and only store it in designated lockers or covered bag racks. Never leave it unattended in a public place.
4. Be *Ready to Learn*: bring your iPad to school fully charged every morning - you won't be able to charge it during the day, nor will you be lent a spare one.
5. Follow instructions: only take your iPad out of your bag when a teacher tells you to and lay it flat on your desk so the screen can be seen. You are not allowed to use messaging, personal apps, or games during lessons. Misuse may result in confiscation.
6. Keep it in the bag: do not use your iPad in corridors, the refectory, or outside unless a teacher has given you specific permission. It can be used in the libraries.
7. Save to OneDrive: Always save your files to OneDrive so your work isn't lost if the iPad malfunctions or something is accidentally deleted.
8. Acceptable Use: Only use the camera with a teacher's permission and never take or post photos of others without their consent. Sound/ music/ notifications should be switched off.
9. Be aware of monitoring: remember that school internet filters still work at home and the iPad will automatically shut down at night to help you sleep.
10. Report problems: if the device is stolen, lost or damaged, report this to the IT Support Desk immediately. If lost, make every effort to find the iPad. A £50 excess and administration fee may be charged to the fee bill. Malicious damage or repeated loss may result in your parents being charged the full replacement cost.