Annemount

Nursery and Pre-preparatory School

Annemount School Online Safety Policy

This policy applies to the whole school including EYFS

This policy should be read in conjunction with the following policies:

Safeguarding Policy
Behaviour and Anti-Bullying Policy
Acceptable Use of ICT for Pupils
Acceptable Use of ICT for Staff
Acceptable Use of ICT for Parents

Contents

Roles and Responsibilities

Handling Incidents

Introduction

Annemount School is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment.

This policy is intended to ensure that:

- Pupils and adults will be responsible users and stay safe whilst using the internet and other communication technologies for educational, personal and recreational use.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Annemount School will endeavour to ensure that pupils will have access to ICT to enhance their learning and will encourage the pupils to be responsible users.

Technology in the Curriculum

Technology has transformed the entire process of teaching and learning at Annemount School. It is a crucial component of every academic subject, and is also taught as a subject in its own right. Classrooms are equipped with electronic whiteboards, projectors and computers. We also have laptops and iPads for use in lessons.

The Role of Technology in our Lives

Technology plays an important part in the lives of all members of our community. Sophisticated games consoles, or PSPs (play stations portable), like Wiis and Nintendo DS, together with Bluetooth-enabled mobile phones provide unlimited access to the internet, to SMS messages, to blogging (web logging) services (like Twitter), to Skype (video calls, via web cameras built into computers, phones and PSPs), to wikis (collaborative web pages), chat rooms social networking sites (such as Facebook) and video sharing sites (such as YouTube).

This communication revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of our role at Annemount to raise awareness to pupils, staff and parents on how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks linked to the potential content, contact and conduct within websites *(Pg. 7)*, including identity theft, bullying, harassment, grooming, radicalisation, stalking and abuse. At Annemount online education is taught at an early age through age appropriate resources, discussions and classroom rules.

Roles and Responsibilities

Head Teacher

- Must be adequately trained in off-line and online safeguarding, in line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance
- To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding
- To take overall responsibility for online safety provision
- To take overall responsibility for data management and information security ensuring school's provision follows best practice in information handling
- To ensure the school uses appropriate IT systems and services including, filtered Internet Service
- To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- To be aware of procedures to be followed in the event of a serious online safety incident
- To receive regular monitoring reports from the IT and Systems Support Technician
- To ensure school website includes relevant information.

ICT Coordinator

- Work alongside the Head Teacher to promote an awareness and commitment to online safety throughout the school community
- Ensure that online safety education is embedded within the curriculum
- Liaise with school technical staff where appropriate

Pupils' use of internet

- Use of the internet, is permitted as directed by the teacher for purposes such as: - research and learning activities directly related to the curriculum.
- Pupils in Reception and KS1 to read, understand, sign and adhere to the **Pupils Acceptable Use Agreement/Policy** *(Appendix 1).*
- The use of game-style activities should be monitored by the teacher to determine suitability. Violent games are NOT permitted.
- Personal e-mail, social networking or instant messaging sites are NOT to be accessed by pupils.
- Pupils should understand the importance of reporting abuse, misuse or access to inappropriate materials
- Pupils should know what action to take if they or someone they know feels worried or vulnerable when using online technology

- Children should report any misuse of the internet to their teacher.
- Personal information such as full names, home addresses, and phone numbers should NOT be shared unless authorised by parents.

Staff use of internet

- Use of the internet on school premises should principally be for school use, e.g. accessing learning resources, educational websites, researching curriculum topics, use of email on school business.
- To read, understand, sign and adhere to the school **Staff Acceptable Use Agreement/Policy** *(Appendix 1)***,** and understand any updates annually.
- Use of the school's internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is excluded.
- Teachers may only access the internet for personal reasons outside school teaching hours.
- Use of the internet to access any illegal sites or inappropriate material is a disciplinary offence. (If accessed accidentally, users should report incident immediately to the Designated Safeguarding Lead and it should be logged.)
- School staff needs to be aware of the importance of maintaining professional standards of behaviour with regard to their own internet use and use of technology, particularly in relation to their communications with parents and pupils.

The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- If personal mobile phones are brought into the school they are stored away in the office and used only during non-contact time.
- Staff may only use their phones in a private staff-only area, i.e. in the staff room, where no pupils are present.
- On school trips, staff should take a mobile with them and use it where phone contact needs to be made. Mobiles should not be used unless unavoidable, i.e. to make a call to the other adult on the trip.
- Staff should always use school equipment to take photographs and only store images on the school computer system.
- Staff should take care regarding the content of and access to their own social networking sites and ensure that pupils and parents cannot gain access to these.

- Staff should not contact the parents or children via personal telephone, email, or social media including Facebook, Instagram, and Twitter or other social networking sites as these may be misinterpreted or taken out of context.
- No reference, text or photos, should be made to work life or to Annemount on any website.
- Staff should ensure that any materials published on their own social networking sites or any website in relation to themselves are neither inappropriate nor illegal, with due consideration shown towards the reputation of their profession.
- Staff should be particularly careful regarding any comments to do with the school or specific pupils that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.
- Staff should ensure that personal data relating to pupils is stored securely on a password-protected computer and password-protected USB if taken off the school premises.
- Staff members who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct.
- It is never acceptable to accept a ‘friendship request’ from pupils or families at the school, as in all cases, children in our school (of KS1 or EYFS age) using such networks will be breaching terms and conditions of use of those networks. If a member of staff has an established connection with an Annemount family prior to employment, this must be disclosed.
- It is also extremely inadvisable to accept as friends ex-pupils who are still minors.
- If a parent of a pupil seeks to establish contact, the member of staff should exercise their professional judgement and inform the Head.

Parents/Carers

- To read, understand and promote the school’s **Pupil Acceptable Use Agreement** with their child/ren
- To read, understand, sign and adhere to the school **Parent Acceptable Use Agreement/Policy** *(Appendix 1)* and understand any updates annually.
- To consult with the school if they have any concerns about their children’s use of technology
- To support the school in promoting online safety and endorse the Parents’ Acceptable Use Agreement which includes the pupils’ use of the Internet and the school’s use of photographic and video images

Treating Other Users with Respect

- We expect all members of the school community to treat each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The school is strongly committed to promoting opportunities for all, regardless of race, gender, gender orientation or physical disability.
- All members of the community are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issue to a member of staff.
- The cameras, webcam and the camera function on the school iPads may be used by pupils and teachers for educational purposes only under teachers' supervision.

This policy has regard for *DfE Cyberbullying: Advice for headteachers and school staff 2014* as well as *Advice for parents and carers on cyberbullying 2014.*

Systems & IT Support Technician

- To report online safety related issues that come to their attention, to the Head
- To manage the school's computer systems, ensuring
  - school password policy is adhered to
  - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)
  - access controls/encryption exist to protect personal and sensitive information held on school-owned devices
  - the school's policy on web filtering is applied and updated on a regular basis
- That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Head Teacher
- To ensure appropriate backup procedures and disaster recovery plans are in place
- To keep up-to-date documentation of the school's online security and technical procedures

Data security

At this school:

- We ensure staff know how and whom to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record
- All servers are in lockable locations and managed by DBS-checked staff.

Use of portable computer systems, USB sticks or any other removable media

- Laptops are the property of the school and are for delivering school work.
- Family and friends are not permitted to use the school laptop provided for the teacher's use.
- Staff members are responsible for maintaining the secrecy of school passwords and these should not be divulged to anyone else (including colleagues, pupils or members of their family).
- Staff will be held responsible for any misuse of the laptop issued to them.
- All sensitive data, such as children's personal details and reports, should be stored on a password protected storage device.

Use of mobile phones on site

- Staff mobile phones are to be stored in the office during teaching hours.
- Staff should NOT use their personal phones for school business or for taking photographs of children. Unless, in exceptional circumstances, an emergency telephone call needs to be made.
- Mobile phones should not be used when teaching.
- Pupils should NOT bring mobile phones to school.
- Parents and Visitors are asked to keep mobile phones on silent and not to use cameras when on the school premises or volunteering with school trips, unless given permission.

Use of digital images

- Images of pupils are to be stored on the school server only.
- Personal photographs will not be stored on school laptops.
- Any photos or videos taken by teachers, other adults (including parents), and the children themselves during ANY school activity (including trips / camp) should not be put on public display or published anywhere on the internet (including social networking sites such as Facebook) unless agreed by the Head from school promotion such as the School Website.

Misuse: Statement of Policy

We will not tolerate any illegal material, and will always report illegal activity to the police and/or the Local Child Safeguarding Board (LCSB). If we discover that a child or young person is at risk as a consequence of online activity, we may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). We will impose a range of sanctions on any member of the community who misuses technology to bully, harass or abuse. Notifications will be made to Ofsted in the event of an allegation of serious harm or abuse by any person working in the school or the Early Years setting.

Common Risks likely to Encounter Online

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse;
- lifestyle websites, for example pro-anorexia/self- harm/suicide sites;
- hate sites;
- content validation: how to check authenticity and accuracy of online content;

Contact

- grooming;
- cyber-bullying in all forms;
- identity theft (including ‘frape’ (hacking Facebook profiles)) and sharing passwords;

Conduct

- privacy issues, including disclosure of personal information;
- digital footprint and online reputation;
- health and well-being (amount of time spent online (internet or gaming));
- sexting (sending and receiving of personally intimate images);
- copyright (little care or consideration for intellectual property and ownership (for example music and film)).

Responding to Incidents

All incidents and complaints relating to e-safety and unacceptable use of technology will be reported to the Head who will make a record of it.
E-safety incidents involving safeguarding issues will be reported to the DSL.
Incidents involving the Head Teacher must be reported directly to the LADO.

If a pupil or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen. Teachers should reassure pupils that they have done nothing wrong. The incident should be reported to the Head and details of the website address and URL provided. The Head will liaise with the School's IT support to ensure that access to the site is blocked and the school's web filtering system reviewed to ensure it remains appropriate. It is essential that teachers ensure that where they have asked for filtering to be lifted for a particular lesson that they notify the school's IT support so that filtering can be put back to minimise the risk of inappropriate sites being accessed by pupils or staff.

If a member of staff is aware of the misuse of technology by a colleague, they should report this to the Head immediately. The IT support manager should be informed so that the computer or laptop is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded. Once the facts are established, the head teacher should take any necessary disciplinary action against the staff member and report the matter where appropriate.

Review and Monitoring

The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school

Involvement with Parents and Guardians

We seek to work closely with parents and guardians in promoting a culture of e-safety. We will always contact parents if we have any worries about their child/rens' behaviour in this area, and we hope that they will feel able to share any worries with us. We recognise that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. We therefore arrange occasional parent talks led by the Head Teacher about the potential hazards of this exploding technology, and the practical steps that parents can take to minimise the potential dangers to their child/ren's without curbing their natural enthusiasm and curiosity. The parents receive a copy of the pupils' Acceptable Responsible Use Policy, as well as sign a Parents Acceptable Responsible Use Policy.

Keeping the School Network Safe

- Certain sites are blocked by our filtering system (Smoothwall)
- We have strong anti-virus protection on our network, which is operated by IT Support.
- Staff are unable to download any software from the Internet that can compromise the network, or are not adequately licensed. Any software requests need to be confirmed with IT support.
- Children do not use 3G/4G.

Promoting Safe Use of Technology

All staff, pupils (Reception & KS1) and parents sign an Acceptable Use Policy that sets out their rights and responsibilities and incorporates the school e-safety rules regarding their use of technology.

The safe use of technology is taught to pupils of all ages through Computing and PHSE lessons, presentations, assemblies and discussion in the meetings of the School Council. Particular attention is paid to school practices to help children to adjust their behaviours in order to reduce risks and build resilience, including radicalisation, with particular attention to the safe use of electronic equipment and the internet. These practices are age appropriate and delivered through a planned component of the curriculum. Children should understand the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults.

Date: September 2019
Review: July 2020

Annemount School

ICT Acceptable Use Policy for Staff

As a professional organisation with responsibility for young people's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the schools' computer systems in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

- It should be understood that this Code of Practice is in place to protect staff from potential risk in their use of ICT in their everyday work.
- This Acceptable Use Policy should be read in conjunction with the schools Online Safety Policy.
- Teachers should be familiar with the school Safeguarding Policy.
- Teachers should closely monitor and scrutinise what their pupils are accessing on the internet.
- When pupils are using the internet it should be controlled by a teacher or adult.
- Pupils should be given a clearly defined focus for using the internet or email and taught skills and techniques to enable efficient and effective use of it.
- Software should not be downloaded from the internet (including screen savers, games etc.) or installed by anyone other than IT Support, unless permission has been granted by the Head Teacher.
- All sensitive data, such as children's details or reports, should be stored on an password protected storage device.
- The use of the internet to access any illegal sites or inappropriate material is a disciplinary offence.
- If offensive material is accessed accidentally, the website should be closed immediately and the incident reported to the head teacher and logged.
- Always ensure that when taking and /or publishing images of others, permission has been obtained in accordance with the school's policy on the use of digital/video images and a school camera has been used. Using personal equipment to record these images is not appropriate, unless you have permission to do so, and these photographs will not be shared on the internet or put on public display without permission.
- Teachers should understand that the school use of the internet on school premises should principally be for school use, e.g. accessing learning resources, educational websites, researching curriculum topics, use of email on school business.
- Teachers should not be accessing the internet for personal reasons whilst teaching children.
- The school recognises that many staff will actively use Facebook, Twitter, and other such social networking sites, blogging and messaging services. Staff must not post material (including text or images) which damages the reputation of the

school or which causes concern about their suitability to work with children. Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks.

- Those who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct.
- It is never acceptable to accept a friendship request from pupils at the school, as in all cases, children of KS1 and EYFS age using such networks will be breaching terms and conditions of use of those networks.
- It is also extremely inadvisable to accept as friends ex-pupils who are still minors. If a parent of a pupil seeks to establish contact, the member of staff should exercise their professional judgement.
- Teachers should NOT use their personal phones for school business or for taking photos of children. Mobile phones should not be used when teaching, unless authorised.

I confirm that I have read and understood the Acceptable Use Policy for ICT and agree to abide by it.

Signed ________________________

Print Name ________________________

Date ________________________

Annemount
Nursery and Pre-preparatory School

Annemount School

ICT Acceptable Use for Parents

As a professional organisation with responsibility for young people's safeguarding it is important that all members of the school community take all possible and necessary measures to support children to manage technology safely and effectively. This includes protecting data and information systems from infection, unauthorised access, damage, loss, and abuse and theft as well as sharing personal data including photographs inappropriately.

The school asks that parents help to achieve this by agreeing;

- To promote the school's **Acceptable Use Agreement for Pupils*** with their child/ren*(*Below - children will be discussing this with their teacher in school and signing)*
- To support the school in promoting online safety
- Parents and visitors are asked to keep mobile phones on silent and not to use cameras when on the school premises or volunteering with school trips, unless given permission.
- We expect all members of the school community to treat each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact.
- We expect members of the school community to ensure that any materials published on their own social networking sites has due consideration shown towards the staff, pupils and families of the school.
- Photographs representing pupils of the school may only be posted on personal social media sites with permission from the parents of those children.
- Parents are asked to be vigilant when sharing photographs of their children in school uniform on social media. Any form of identification puts a child at risk.

This policy should be read in conjunction with the schools Online Safety Policy which can be downloaded from the school website or a hard copy obtained from the school office.

I confirm that I have read and understood the Acceptable Use Policy for ICT and agree to abide by it.

Signed ________________________

Print Name ________________________

Date ________________________

*

Annemount School

ICT Acceptable Use for Pupils

Think before you click

S — I will only use the internet and email with an adult

A — I will only click on icons and links when I know they are safe

F — I will only send friendly and polite messages

E — If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

Annemount
Nursery and Pre-preparatory School

Annemount School

ICT Acceptable Use for Pupils

Think before you click

S	I will only use the internet and email with an adult
A	I will only click on icons and links when I know they are safe
F	I will only send friendly and polite messages
E	If I see something I don’t like on a screen, I will always tell an adult

My Name:

My Signature: