# NEWBRIDGE SCHOOL

# E-SAFETY POLICY

# 2017-2018

**OTHER POLICY LINKS**

**Anti-Bullying**

**Data Protection Retention and Security Policy**

**Behaviour Management Policy**

**ICT Acceptable Use**

**Anti-Radicalisation Policy**

**Curriculum Links: PHSE/ICT/Safer Internet Day**

| | |
|---|---|
| **Updated:** | September 2017 |
| **Review Date:** | September 2018 |
| **Staff Responsible**: | E-Safety Co-ordinator & PHSE, Advance Trust ICT Consultant Technician, Newbridge Office Manager |

## Our Vision

Newbridge embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Newbridge School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

## Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and young people while on the school premises.

## Related Documents:

| | |
|---|---|
| Acceptable Use Policy for Adults | (Appendix 3 and 4) |
| Acceptable Use Policy for Young People | (Appendix 2 & 3) |
| Data Protection Retention and Security Policy | |
| Behaviour Management Policy | |
| Anti-bullying Policy | |
| Policy Owner (E-Safety Co-ordinator): | Assistant Headteacher |
| Implementation Date: | September 2010 |
| Updated: | September 2017 |
| Review Date: | September 2018 |

## Publicising e-Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website.
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated.
- Post relevant e-Safety information in all areas where computers are used.
- Provide e-Safety information at induction meetings for all families.

## Roles and Responsibilities

The Head and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our school.

The role of ***e-Safety co-ordinator*** has been allocated to, our designated senior person for child protection and a member of the senior management team. They are the central point of contact for all e-Safety issues and will be responsible for day to day management. The school has established an e-Safety committee that are responsible for policy review, risk assessment, and e-safety in the curriculum. The current members are:

- Assistant Headteacher, E-Safety Co-ordinator & PHSE
- Advance Trust ICT Consultant Technician
- Newbridge Office Manager

All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly.
- Accept responsibility for their use of technology.
- Model best practice when using technology.
- Report any incidents to the e-Safety coordinator using the school procedures.
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action.

Additional roles and responsibilities are discussed in the Becta document - AUP's in context: Establishing safe and responsible behaviours http://publications.becta.org.uk/display.cfm?resID=39286 . These will be communicated to the relevant groups at appropriate times.

## Physical Environment/Security

- The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with Advance Trust ICT Consultant Technician where appropriate.
- Anti-virus software is installed on all computers and updated regularly.
- Central filtering is provided and managed by **Advance Trust**. All staff and students understand that if an inappropriate site is discovered it must be reported to the e-Safety co-ordinator who will report it to ***Advance Trust ICT Consultant Technician.***
- All incidents will be recorded in the e-Safety log for audit purposes.
- Pupils use is monitored by Advance Trust ICT Consultant Technician using Forensic software.

- Staff use is monitored by the Headteacher and Advance Trust ICT Consultant Technician.
- All staff are issued with their own username and password for network access.
- All pupils are issued with their own username.

**Mobile/emerging technologies**

- Teaching staff at the school are provided with a laptop for educational use and their own professional development. All staff understand that the *Acceptable Use Policies* apply to this equipment at all times.
- School mobile phones are issued to staff that may be contacted by pupils or parents.
- To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network.
- Staff understand that they should use their own mobile phones sensibly and in line with school policy.
- Pupils understand that their mobile phones must be handed into Student Reception for safe keeping.
- The Educations and Inspections Act 2006 grants the Headteacher the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Headteacher will exercise this right at their discretion.
- Pictures/videos of staff and pupils should not be taken on personal devices.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community.

**E-mail**

The school e-mail system is provided, filtered and monitored by **Advance Trust**.

All staff are given a school e-mail address and understand that this must be used for all professional communication.

- All pupils are given a school e-mail address that can be used for educational purposes.
- Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication.
- Guidance is given to the school community around how e-mail should be structured when using school e-mail addresses.
- Staff are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software.
- Pupils may be given the opportunity to check their own e-mail outside directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software.
- Everyone in the school community understands that any inappropriate e-mails must be reported to the class teacher/e-Safety Co-ordinator as soon as possible.

## Published Content

The Headteacher takes responsibility for content published to the school web site but delegates' general editorial responsibility to a nominated staff member. Class teachers and Key Stage co-ordinators are responsible for the editorial control of work published by their students.

- The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution. *(To be added as part of process of moving to learning platforms)*
- The school encourages the use of e-mail to contact the school via the school office, generic e-mail addresses & staff e-mail addresses.
- The school does not publish any contact details for the pupils.
- The school encourages appropriate, educational use of other Web technologies and where possible embeds these in the school web site or creates a school account on the site.

## Digital Media

We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or video are published or distributed outside the school. **(see Appendix 1)**

- Photographs will be published in line with Becta guidance and not identify any individual pupil.
- Students' full names will not be published outside the school environment.

## Social Networking and Online Communication

The school is reviewing the use of social networking sites and online communication and currently does not allow access to such sites.

Guidance is provided to the school community on how to use these sites safely and appropriately is given to pupils through termly E-safety weeks. This includes:

- not publishing personal information
- not publishing information relating to the school community
- how to set appropriate privacy settings
- how to report issues or inappropriate content

Pupils are given age appropriate advice and guidance around the use of such sites.

## Educational Use

School staff model appropriate use of school resources including the internet.

- All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material.
- Where appropriate, links to specific web sites will be provided instead of open searching for information.
- Students will be taught how to conduct safe searches of the internet and this information will be made available to parents and carers.
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Policy before any activity.
- Staff and students will be expected to reference all third party resources that are used.

## E-safety Training

The school have completed a baseline assessment of current staff skills and have a program of continuing professional development in place that includes whole school inset, in school support, consultancy and course attendance.

- There is an induction process and mentor scheme available for new members of staff.
- E-Safety is embedded throughout the school curriculum and visited by each year group.
- Pupils are taught how to validate the accuracy of information found on the internet.
- Parents are directed at a child's Induction to the availability of E-safety training & support appropriate to their needs.

## Data Security/Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998.

Data is stored on the school systems and transferred in accordance with the Becta Data Security Guidelines.

## Wider Community

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and password that will be recorded in the school office.

## Equal Opportunities

Please refer to our Equal Opportunities Policy.

## Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Child Protection Policy.

- Any suspected illegal activity will be reported directly to the police.
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head.
- Breaches of this policy by staff will be investigated by the head teacher. Action will be taken under the ***Advance Trust's Guidelines on the use of Disciplinary Procedures policy*** where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All monitoring of staff use will be carried out by at least 2 senior members of staff.
- Student policy breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the nominated child protection representative and action taken in line with school anti-bullying and child protection policies. There may be occasions when the police must be involved.
- Serious breaches of this policy by students will be treated as any other serious breach of conduct inline with school Behaviour Policy. Referral to Heads of Phase may be appropriate at this level. Heads of Phase will also deal with email alerts generated by PCE for students. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.
- Minor student offenses, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school behaviour policy.
- The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate.

**Appendix 1**

**MEDIA/SCHOOL PARENTAL PERMISSION FORM**

To celebrate events in the School we may invite the press to take photographs of the children for publication. Examples of this include projects undertaken in the School.

To ensure that we comply with parent's wishes on these matters, please complete this form so we have a record of your views.

I give permission for my child's photograph to appear in the School. **YES/NO**

I give permission for my child's photograph to appear in a newspaper report of any event at school. **YES/NO**

I give permission for my child's first name to be printed in a newspaper report of an event at school. **YES/NO**

I give permission for my child's full name to be printed in a newspaper report of an event at school. **YES/NO**

**Child's signature**: …….

**Parent's signature**: …….

**Date**: …….

**Appendix 2**

**INTERNET PERMISSION FORM**

Name of Child……..

As part of the School 's Information and Communication Technology (ICT) programme we offer supervised access to the internet.

The Pupils will be supervised at all times while they are using this resource; however, I want you to be aware that slip-ups are a possibility. I therefore require your written permission for your son/daughter to use this facility and that we cannot be held responsible for their misuse.

I am happy to allow my child to use the Internet and agree to the AUP for:

Child's signature: …….

Parent's signature: …….

Date: …….

Acceptable Use Policy

*I want to feel safe all the time.*

*I agree that I will:*

- only visit sites which are appropriate to my work at the time
- work in collaboration only with friends and I will deny access to others
- tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
- make sure all messages I send are respectful
- show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend
- only email people I know or those approved by a responsible adult
- only use email which has been provided by school
- talk to a responsible adult before joining chat rooms/network sites
- always keep my personal details private. (e.g. My name, family information, journey to school, my pets and hobbies )
- always check with a responsible adult and my parents before I show photographs of myself
- never meet an online friend without taking a responsible adult that I know with me

*I know that once I post a message or an item on the internet then it is completely out of my control. I know that anything I write or say or any website that I visit may be being viewed by a responsible adult.*

**Appendix 3**

**Acceptable use policy for all adults working with children**

This policy aims to ensure that any communications technology is used without creating unnecessary risk to users while supporting learning.

*I agree that I will:*

- Only use personal data securely.
- Educate pupils in the effective use of the internet e.g. research, retrieval & evaluation.
- Educate pupils in the recognition of bias, unreliability & validity of resources
- Only use approved e-mail accounts.
- Only use pupil images or work when approved by parents & in a way that individual children cannot be identified.
- Only give access to appropriate users when working with e.g. internet, e-mail.
- Use and support the white list filtering system in place.
- Report unsuitable content or activities to the E-Safety Co-ordinator.
- Read & sign the acceptable use policy.
- Pass on any examples of Internet misuse to a senior member of staff
- Should any adult encounter any inappropriate material accidentally, they are expected to report it immediately. Thus enabling the filtering service to block any further access.
- No program files may be downloaded to the computer from the Internet. This is to avoid viruses.
- No personal information such as phone numbers & addresses should be given out & no arrangements to meet someone made.

*I know that once I post a message or an item on the internet then it is completely out of my control.*

*I know that anything I write or say or any website that I visit may be being viewed by a responsible adult. I agree that I will not:*

- visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - pornography (including child pornography)
  - promoting discrimination of any kind
  - promoting racial or religious hatred
  - promoting illegal acts
  - breach any Local Authority/School policies, e.g. gambling
  - do anything which exposes children in my care to danger
  - any other information which may be offensive to colleagues
- forward chain letters
- breach copyright law

*I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.*

Staff Signature: ……..... Date: ……

**Appendix 4**

## Acceptable Use Policy for Governors

*The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.*

***The governors will ensure that:***

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning;
- learners are made aware of risks and processes for safe digital use;
- all adults and learners have received the appropriate acceptable use policies and any required training;
- the school has appointed an e-Safety Coordinator and a named committee member takes responsibility for e-Safety;
- an e-Safety/Internet Policy has been written by the school, building on the LSCB e-Safety Policy and BECTA guidance ;
- the e-Safety/Internet Policy and its implementation will be reviewed annually;
- the school internet access is designed for educational use and will include appropriate filtering and monitoring;
- copyright law is not breached;
- learners are taught to evaluate digital materials appropriately;
- parents are aware of the ICT Acceptable Use Policy;
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text;
- the school will take all reasonable precautions to ensure that users access only appropriate material;
- the school will audit use of technology (using the Self-Review Framework) to establish if the e-safety policy is adequate and appropriately implemented;
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff.