Normanton Junior Academy

TOGETHER WE LEARN

Normanton
Junior Academy

E-Safeguarding Policy

Introduction

New technologies have revolutionised the movement, access and storage of information with important implications for all schools. Use of ever more powerful computers, iPads, broadcast media, the Internet, digital recorders of sound and images together with increased opportunities to collaborate and communicate are changing established ideas of when and where learning takes place. At Normanton Junior School we recognise that learning is a lifelong process and that e-learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. The school is committed to the continuing development of our ICT infrastructure and embracing new technologies so as to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. E-safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks.

This policy applies to all stakeholders of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. This policy has been developed to ensure that all stakeholders are working together to safeguard and promote the welfare of children. E-Safeguarding is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of E-safeguarding at all times, to know the required procedures and to act on them. Safeguarding and promoting the welfare of pupils needs to be embedded into the culture of the school and its everyday practice and procedures. All staff have a responsibility to support E-Safeguarding practices in school. Concerns related to child protection will be dealt with in accordance with the school's Safeguarding Policy and should be reported to the designated persons.

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the e-safeguarding risks. This policy will regularly be amended to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an E-Safeguarding risk.

The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but which are linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles & Responsibilities
The SLT will (ensure):

- *All* staff are included in E-Safeguarding training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A Designated Senior Member of Staff for E-Learning/Safety is identified (Iain Clarke) and receives appropriate on-going training (ICT network meetings) support and supervision and works closely with the Designated Governor for Safeguarding (Mark Winn).
- All temporary staff and volunteers including students are made aware of the school's E-Safeguarding Policy and arrangements.
- A commitment to E-Safeguarding is an integral part of the safer recruitment and selection process of staff and volunteers.
- The Headteacher is designated as the Senior Information Risk Officer (SIRO) to assess the risk of the use of different types of technology and information data sets that are owned by the school.
- The SIRO board consists of The Head (Trudie Southward), The ICT Leader (Iain Clarke), The School Business Manager (Alison Waddington) and the Chair of Governors (Mark Winn)
- An E-Safeguarding culture will be promoted within the school community.
- The ICT Co-ordinator will receive training and support in their work leading E-Safeguarding in school.

The Governing Body of the school will ensure that:

The Governors of the school are responsible for the approval of this E-Safety Policy and for reviewing the effectiveness of the policy. This is carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor includes:

- regular meetings with the IT Leader
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to the Governing Body

The Designated Member of Staff for E-Safeguarding and ICT will:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for E-Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff, governors and volunteers on E-Safeguarding.
- Check that all Staff, governors and visitors read and sign the schools acceptable use agreement
- Ensure that all staff and volunteers understand and are aware of the school's E-Safeguarding policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated. Any mobile devices such as laptops or ipads will be connected to the school's networks for updating purposes on a regular basis.
- Discuss security strategies with the LA particularly where a wide area network is planned.
- Promote E-Safeguarding education across the curriculum in the school and to parents/carers.
- The Senior Information Risk Officer (SIRO) has carried out appropriate risk assessments dealing with the use of ICT equipment and technologies and the information data sets owned by the school.
- Ensure that an E-Safeguarding incident log is kept up-to-date and regularly monitored/reviewed termly by the E-Safeguarding team (E-Safeguarding coordinator, ICT Leader, SIRO if different from the E-Safeguarding coordinator, ICT technician and where possible a designated member of the governing body)

- Ensure that the use of the network, remote access and email are regularly monitored in order that any misuse or attempted misuse can be reported to the Designated Lead for Safeguarding and E-Safety for investigation, action, or sanction
- Ensure that the Designated Lead for Safeguarding is trained in e-safety issues and is aware of the potential for serious child protection issues to arise from:
- sharing of personal data
- access to illegal or inappropriate materials
- inappropriate on-line contact with adults and strangers
- potential or actual incidents of grooming
- cyber-bullying

Teachers and Support Staff will:

- Read, understand and help promote the school's E-Safeguarding policies and guidance.
- Read, understand and adhere to the school staff AUP.
- Develop and maintain an awareness of current E-Safeguarding issues and guidance.
- Model safe and responsible behaviours in your own use of technology.
- Embed E-Safeguarding messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Be aware of what to do if an E-Safeguarding incident occurs.
- Maintain a professional level of conduct in their personal use of technology at all times.
- Ensure that in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

The ICT Technician will:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

Parent and Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and information about national and local e-safety campaigns and literature.

- Parents/carers will be informed of the school's Internet Policy which can be accessed via the school website and in the school brochure.
- Any issues concerning the internet will be handled sensitively to inform parents/carers without undue alarm.
- Advice on filtering systems and appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/carers via the website.
- A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.
- Parents/ carers will be expected to agree and sign the home/ school agreement which clearly states the use of photographic and video images outside of school.

Teaching and learning

The internet is an important part of the statutory curriculum and a necessary tool for staff and children. The internet benefits education by allowing access to world - wide educational resources. The school Internet access is designed expressly for pupil and educational use. All internet access shall be filtered for inappropriate images and websites in accordance with the local authority, YHGfL and Internet Watch Foundation (IWF) policies. Children are taught what Internet use is acceptable their responsible internet use rules displayed in the ICT suite. Clearly planned learning objectives for using the Internet are shared with the children before the session and pupils are taught how to safely search for internet content of all types (images, information, video, music etc.) in order to further their learning. The school will provide a series of specific E-Safeguarding related lessons in every year as part of the ICT curriculum / SEAL curriculum. We will celebrate and promote E-Safeguarding through a planned programme of assemblies and whole-school activities. We will discuss, remind or raise relevant E-Safeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials. A section on the school website will give parents information on how to keep their children safe on the internet.

Managing passwords

Passwords are an important part of computer security, they are a form of authenticating a user against a given username. At Normanton Junior School pupils use passwords of varying complexity linked to their age. (Y3 no password, Y4 simple password, Y5 to include a capital letter, Y6 to include a capital letter and number)

- Staff are reminded that usernames and passwords should not be shared with other members off staff
- All staff are forced to change their passwords periodically under the guidance of the ICT manager, these passwords have to include a capital letter and number.

Managing internet access

- The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
- The school internet access is designed expressly for educational use and will include filtering appropriate to the age of the children and young people.
- All users will sign an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using the school ICT systems, and that such activity will be monitored and checked
- Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use through the 'Responsible internet use' displays and in ICT lessons and assemblies delivered by the ICT co-ordinator. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.
- Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening (See whole school ICT display)
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider (Wakefield Local Authority) and filtration providers (YHGfL) via the E-Safeguarding Co-ordinator. Any incidents relating to unsuitable sites/content should be documented within the E-Safeguarding Incident Management log.

Managing email

- Incoming e-mail should be monitored by the class teacher and attachments should not be opened unless the author is known.
- Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.
- Access in school to external personal e-mail accounts may be blocked (At the discretion of the headteacher and designated E-Safeguarding lead teacher).
- Staff sending any work related communications will always utilise a school email address (Never a personal email account) Consideration will be given to the types of content sent to external third parties at all times (e.g sending pupil information etc.)
- Staff are reminded to avoid sending sensitive data via email. Any data deemed sensitive sent by email will be password protected or encrypted and the email address checked by a colleague.

Managing school website content

- Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.
- Photographs of pupils will not be used without the written consent of the pupil's parents/carers.
- The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- The Headteacher or nominated person (Iain Clarke) will have overall editorial responsibility and ensure that all content is accurate and appropriate.
- The website will comply with the school's guidelines for publications and parents/carers will be informed of the school's policy on image taking and publishing.
- Use of site photographs will be carefully selected so that pupils cannot be identified or their image misused. The full names of pupils will not be used on the website, particularly in association with any photographs.
- Work will only be used on the website with the permission of the pupil and their parents/carers.
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Filtering

- The school will work in partnership with parents/carers; the Local Authority, the DFE and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.
- **ALL** internet usage will be monitored for inappropriate use.
- If staff or pupils discover unsuitable sites, the URL and content must be reported and the E-Safeguarding Co-ordinator.
- Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk) the local authority and YHGfL.
- Regular checks by Senior Staff will ensure that the filtering methods selected are appropriate, effective and reasonable.
- The level of filtering and content available will be selected by the school in conjunction with the LA and will be age and curriculum appropriate.

Managing digital content

Camera & Images (this should be referenced alongside appendix 2)

- Written permission from parents or carers will be obtained for the following areas before photographs of pupils are published. This will be done annually or as part of the induction process on entry to the school:

- ➢ On the school website
- ➢ In display material that may be used around the school
- ➢ In display material that may be used off site
- ➢ Recorded or transmitted on a video or via webcam in an educational conference
- ➢ Media publications.

Staff will:

- follow school policies concerning the sharing, distribution and publication of images. Images should only be taken on school equipment. Personal equipment of staff should not be used for such purposes.
- ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- ensure that pupils do not take, use, share, publish or distribute images of others without their permission .
- ensure pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Parents:

- Parents and carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.
- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- Parents may take photographs at school events however they must ensure that any images or videos taken, involving children other than their own, are for personal use and will not be published on the internet including social networking sites

Storage of images

- Any photographs/video of children should be taken using school owned devices. All data images situated on camera internal storage should be removed on a regular basis.
- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- The use of cloud based programmes (such as One Drive) to store images is not permitted to comply with DPA.
- We will store images of pupils that have left the school for 5 years for use in school activities, promotional resources.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.
- The school ICT technician and ICT co-ordinator have the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

Use of mobile devices (this should be referenced alongside appendix 1)

- Children should not bring mobile phones or devices on to the premises, or on school trips. Any mobile device found by staff will be stored at the office until the end of the day.
- Visitors to the school are asked to switch off their phones before entering the building by the office staff.
- Staff are allowed to bring mobile phones onto the school premises. These have to be stored with personal belongings out of reach of pupils. Staff under no circumstance should be using their mobile phones during lesson times especially when working with pupils. Staff should make mobile communications in a safe place away from children, such as the meeting room or the staff room during the school day. Staff are not permitted to take photographs of children on their mobile phones for security reasons.
- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

Social networking, social media and personal publishing

- Staff using social media websites such as Facebook and Twitter will not bring the school or their own professional status into disrepute.
- Guidance on security settings for Facebook and other sites is available from the E-Safeguarding Coordinator or the YHGFL website
- Staff are acutely aware of the risks of adding pupils/parents as friends.
- Staff will not discuss any element of their professional lives or matters concerning Normanton Junior School on social media sites.

Emergent technologies

New and emerging technologies are being developed constantly in today's fast-moving digital world. These technologies can be anything from handheld devices to new faster communication mechanisms. Schools should try and always be aware of new and appealing technologies as these can, in many cases, offer the potential to develop new teaching and learning tools, including mobile communications, internet access, collaboration and multimedia tools.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out, before use in school is allowed.
- All new technologies will be tested and reviewed for any security vulnerabilities that may exist. Suitable countermeasures will be adopted within school to ensure risks are reduced to an acceptable level.
- Emerging technologies can incorporate software and hardware products.

- The school will periodically review which technologies are available within school for any security vulnerabilities that may have been discovered since deployment.
- All new technologies deployed within school should be documented within the E-Safeguarding and Acceptable Use Policies prior to any use by any member of staff or pupil.
- The acceptable use of any new or emerging technologies in use within school will be reflected within the school E-Safeguarding and Acceptable Use policies.
- Prior to deploying any new technologies within school, staff and pupils should have appropriate awareness training regarding safe usage and any associated risks.

Data Protection

Normanton Junior School has a current registration for data protection. As a commitment to this registration they will be complying with the Data Protection Act 1988, with guidance from their local authority.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Examples of good practice include

.

- Staff ensuring they properly log-off from a computer terminal after accessing personal data.
- Staff locking workstations they are logged on when they are leaving the devices unattended
- Staff not removing personal or sensitive data from the school premises without permission of the Headteacher, and without ensuring such data is kept secure.
- Users being vigilant when accessing sensitive or personal information on screen to ensure no one else, who is unauthorised, can read the accessed information.
- All access to information systems being controlled via a suitably complex password.
- Staff and pupils not leaving personal and sensitive printed documents on printers within public areas of the school.
- All physical information being stored in controlled access areas.
- Fax machines will be situated within controlled areas of the school.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All personal and sensitive information taken offsite being secured through appropriate technical controls, e.g. encrypted full disk, encrypted removable media, remote access over encrypted tunnel.

- All devices taken offsite, e.g. laptops, tablets, removable media or phones being secured in accordance with the school's information-handling procedures and, e.g. not left in cars etc.
- When disposing of equipment all disks and drives being erased to ensure no sensitive information remains on hard disk or storage of any kind
- Physical information sources any documents containing confidential information being shredded within school.

Role of the SIRO

- Any access to personal and sensitive information should be assessed and granted by the SIRO.
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO.
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO.
- The school uses a third party service provider to operate a 'Call parents' service. Parents must consent to be contacted via 'Call parents' they must also be made aware that this service is operated by a third party but their personal information will only be used for this service. Parents have the right to withdraw at any time.
- CCTV cameras are provided and serviced by the company Microlink. All footage, however, is recorded internally on the school's own recording equipment.

Responding to incidents of misuse - Staff

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

then the staff responsible will be subject to disciplinary procedures and dealt with through the Local Area Designated Officer procedures. If any staff member suspects illegal activity, it must be reported immediately to the Designated Lead for Safeguarding and E-Safety, or direct to the Head Teacher. The matter must not be discussed with any other member of staff under any circumstances. If there is a breach of the E-Safety policy that is not considered illegal then the matter will be dealt with appropriately and proportionately. Continuous breaches of the policy will result in serious disciplinary procedures by the Head Teacher

Pupils

All staff are responsible for ensuring that pupils respect and adhere to the E-Safety policy. If any member of staff witnesses or is informed of pupils who are deliberately trying to access material that could be considered illegal or taking part in the activities listed below, it must be reported to a member of the senior leadership team immediately.

- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone, digital camera and other handheld devices
- Unauthorised use of social networking, instant messaging and personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords
- Attempting to access or accessing the school network, using another student's / pupil's account
- Attempting to access or accessing the school network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements of the above, following previous warnings or sanctions

- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school including online bullying or messaging through social media.
- Using proxy sites or other means to subvert the school's filtering system
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

Dealing with complaints

- Staff, children and parents/carers must know how to report incidents to the Headteacher. Concerns related to Safeguarding issues must be dealt with through the school's Safeguarding Policy and Procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- All E–Safety complaints and incidents will be recorded by the school, including any actions taken.
- The school's designated person for E-Safeguarding will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Headteacher immediately. Any misuse will be logged electronically.
- Parents/carers and pupils will work in partnership with the school staff to resolve any issues.
- Sanctions for misuse for pupils may include any or all of the following:

Discussion with the Headteacher
Informing parents/carers
Removal of internet access for a specified period of time

Through all these measures we hope that children have a positive experience when using the internet and that ICT can be used as a tool to further development and teach vital life skills allowing children to make a positive contribution.

This policy refers to the following policies.

- Safeguarding
- Child Protection
- Data Protection Act 1998
- Safe recruitment and selection of staff.

Inclusion

The policy will be applied to all pupils. We welcome our general responsibilities under the Disability Equality Duty by promoting equal opportunities, eliminating discrimination and improving access to learning for disabled people. In order to comply with the requirements of the DDA 2006 we will make reasonable adjustments to ensure all stakeholders understand and can follow this policy. We will actively seek to remove any barriers to learning and participation that may hinder or exclude individuals or groups of pupils.

Monitoring and Review

This policy is monitored by the Headteacher, who reports to governors about the effectiveness of the policy on request. It will be reviewed appropriate to new legislation or to the needs of the school by the schools ICT co-ordinator, assessed each September or as required. Any changes will be disseminated to staff and governors via awareness training.

Date for review-September 2016

Signed …………………………………………………………Headteacher
……………………………………………………………….Chair of Governors