E-Safety Policy

Reviewed annually

Normanton Common Primary Academy

E-Safety Policy

(See also Safeguarding & Child Protection Policy and Anti-Bullying Policy)

Normanton Common Primary Academy uses the DFE document 'Teaching Online Safety in School- (June 2019), to support the work we do with children in school.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

For reporting online concerns please go to – National Crine Agency's Click CEOP reporting service.
Useful advice can also be found through organisations such as
Childline,
NSPCC
The Internet Watch Foundation

Introduction

Normanton Common Primary Academy fully recognises the contribution it can make to protect children and support them in school. The aim of this policy is to safeguard and promote our pupils' safe use of the internet and electronic communication technology.

The internet and other technologies have an important role in the learning and teaching processes, however we feel it is important to balance those benefits with an awareness of the potential risks. This policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

The school acknowledges e-safety and e-security as important issues for our school community and has made a considered attempt to embed e-safeguarding into our teaching and learning. We have considered the wider implications of e-safeguarding beyond classroom practice such as security and data.

This policy applies to the whole school community including the Senior Leadership Team, ASC (Academy Standards Committee), all staff employed directly or indirectly by the school and all pupils. The school's senior leadership team and school ASC will ensure that any relevant or new legislation that may impact upon the provision for E-Safeguarding within school will be reflected within this policy. 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 upon them. Safeguarding and promoting the welfare of pupils needs to be embedded in the culture of the school and its everyday practices and procedures. All staff have a responsibility to support E-safeguarding practises in school. Concerns related to child protection will be dealt with in accordance with the school's Child Protection and Safeguarding Policy and should be reported to designated persons. (Listed at the end of this document).

Many of our pupils will use mobile phones, tablets and computers on a daily basis. They are a source of fun, entertainment, communication and education. However, we know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive communications, to enticing children to engage in sexually harmful conversations, webcam photography, encouraging radicalisation or face-to-face meetings. The school's e-safety policy explains how we aim to keep pupils safe in school, which includes reasonable filters and monitoring. Cyberbullying and sexting by pupils, via texts and emails, will be treated as seriously as any other type of bullying and in the absence of a child protection concern will be managed through our anti-bullying and confiscation procedures.

Chatrooms and some social networking sites are the more obvious sources of inappropriate and harmful behaviour and pupils are not allowed to access these sites in school. Some pupils will undoubtedly be 'chatting' outside school and are informed of the risks of this through PSHE/SRE. Parents are encouraged to consider measures to keep their children safe when using social media.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• **contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Pupils will be educated in online safety, and regularly reminded, as an ongoing part of our curriculum.

Acceptable IT use for staff and pupils will be enforced and parents are also informed of expectations.

To protect students from mobile technology accessing 3G and 4G we will have a ban on mobile phones whilst in school.

Effective Practice in E-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented E-Safety Policy;
- Secure, filtered broadband;
- The use of e-safety control software monitoring system which monitors and captures inappropriate words or web sites used.

Our Aims

- To set out the key principles expected of all members of the school community at Normanton Common Primary Academy with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Roles and Responsibilities

Responsibilities of the school community

We believe that e-safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching.

The SLT will ensure

- The staff are included in E-safety training.
- That staff understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- All temporary staff and volunteers including students are made aware of the school's E-safety policy arrangements.
- The Computing leader will receive training and support in their work leading / e-safeguarding in school.
- That the school Acceptable Use policies are current and pertinent
- That the Designated leader 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, inappropriate online contact with adults and strangers, potential or actual incidents of grooming, cyber bullying

The Headteacher is ultimately responsible for e-Safeguarding provision including eSafeguarding for all members of the school community

The ASC (Academy Standards Committee) 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 ASC receiving regular information about e-safety incidents and monitoring reports.

The designated Member of Staff for E-Safety and ICT/Computing, responsibilities include:

- To promote an awareness and commitment to E-safety throughout the school
- To be the first point of contact in school on all E-safety matters (alongside school DSLs)
- To take day-to-day responsibility for E-safety within school and to have a leading role in establishing and reviewing the school E-safety policies and procedures
- To communicate regularly with school technical staff
- To communicate regularly with the designated Safeguarding governor
- To ensure that all members of staff receive an appropriate level of training in E-safety issues
- To ensure that E-safety education is embedded across the curriculum
- To ensure that E-safety is promoted to parents and carers
- To ensure that all staff are aware of the procedures that need to be followed in the event of an E-safety incident
- To ensure that an E-safety incident log is kept up to date

Teacher and Support Staff responsibilities include:

- To read, understand and help promote the school's e-safety policies and guidance
- To read, understand, sign and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the DSL's via the yellow cause for concern forms – these will be recorded on CPOMS as an eSafety incident
- To develop and maintain an awareness of current e-safety issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, **NEVER** through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed e-safety messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To be aware of e-safety issues related to the use of mobile phones, cameras and handheld devices
- To maintain a professional level of conduct in personal use of technology at all times

The ICT Technician will:

- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure 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.
- Keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others on relevant.

Parents and Carers

- Will be informed of the schools e-safety policy which can be accessed via the school website.
- Will be informed of any issues concerning the internet / websites / games
- Will support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school.
- Will be offered advice on filtering systems and appropriate educational and leisure activities including responsible use of the internet will be provided through leaflets and via the school website.
- Will be expected to comply with the school's policy on the use of photographic and video images outside of school.

Responsibilities of pupils

- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home (with adult support as appropriate to their age group)
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will ensure that e-safety is an integral theme throughout our school curriculum.
- We will provide a series of specific e-safety-related lessons in specific year groups as part of the ICT/computing curriculum / PSHE curriculum.
- We will celebrate and promote e-safety through whole-school activities, including promoting Safer Internet Day.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.

- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member.

Managing Passwords

Passwords are an important part of computer security, they are a form of authenticating a user against a given username.

- Staff are reminded that usernames and passwords should not be shared with other members of staff.
- All staff are asked to change their passwords periodically under the guidance of the Computing lead.

Managing Internet access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- The school internet access is designed expressively for educational use and will include filtering appropriate to the age of the children.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- All staff, volunteers and students will sign an Acceptable Use Policy provided by the school. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.
- Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

Managing email

- Incoming e-mails 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 email.
- Access at school to external e-mail accounts may be blocked (At the discretion of the headteacher and designated e-safty/computing lead teacher)
- Staff sending any work related communications will always utilise a school email address (never a personal email account) Consideration will always be given to the types of content sent to external third parties at all times (e.g sending pupil information etc). Sensitive information should include encrypt in the subject part of the email so it is encrypted as an added security.

Managing school website content and Twitter content

- Photographs of pupils will not be used without the written consent of the pupils parents/carers
- The point of contact on the school website and Twitter will be the school address, email and telephone number. Staff or pupils' home information will not be published.
- The headteacher or nominated person will have overall editorial responsibility and ensure the content is accurate and appropriate.
- Work will only be used on the website or Twitter with the permission of the pupil and their parent/carers.
- The copyright of all material must be held by school.

Filtering

- The school will work in partnership with parents/carers; the Local Authority, the DFE, the Internet Service Provider and MINT 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 to the e-safety/computing lead / DSL's
- Regular checks by MINT will ensure that the filtering methods selected are appropriate, effective and reasonable.
- We filter out social media, such as Facebook.
- Searched and web addresses are monitored and the ICT technicians will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found.

Managing digital content

Camera and images

Written permission form parents or carers will be obtained for the following areas before photographs of pupils are published.

1. On the school/ Trust website/Twitter
2. In display material that may be used around school
3. In display material that may be used off site (e.g. by Waterton Academy Trust)

Storage of images

- Any photograph/video of children should be taken using school owned devices. All data images on a camera or internal storage should be removed on a regular basis.
- Staff are allowed to bring mobile phones on to the school premises. These have to be stored out of reach of children. Staff should only mobile communications in a safe place away from children and only with permission from the headteacher if during the school day (e.g.to make an appointment at break time or lunchtime or when expecting an emergency call).
- Staff are not permitted to use their own personal phones for contacting children or their families within or outside of the setting in a professional capacity.

Social networking, social media and personal publishing

- Staff using social media websites will not bring school or their own professional status into disrepute.
- Staff are accurately aware of the risks of adding pupils/parents as friends.
- Staff will not discuss any element of their professional lives or matters concerning Normanton Common Primary Academy on social media sites
- The senior leadership team will act upon anything they find on social media posted by staff or parents, which they feel would bring the school into disrepute, or its pupils into danger.

Data Protection

Please also see Waterton Academy Trust – Data Protection Policy - https://watertonacademytrust.org/userfiles/files/embeds/data-protection-policy-15e68e41b7ab31.pdf

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.

- Encrypt or password protect any email containing personal data
- Delete any data from a device, in line with the school policy once it has been transferred or its use is complete
- Must not leave personal and sensitive printed documents on printers within public areas of the school
- Dispose of equipment safely e.g. all drives to be erased ensuring no sensitive information remains on the hard disk or storage of any kind (with support from MINT to ensure that this has been done safely and securely)
- Shred any documents which contain confidential information
- Report any data breach to the headteacher who will then report this to Waterton Academy Trust

Responding to issues of misuse –Staff

It is hoped that all members of the school community will be responsible users of IT, 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:

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
- Criminal racist material

Then the staff responsible will be subject to disciplinary and dealt with through the Local Area Designated Officer Procedures. If any staff member suspects illegal activity, it must be reported immediately to the Headteacher (Lead DSL). The matter must not be discussed with other members 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 proportionally.

Dealing with complaints

- Staff, parents and carers must know how to report incidents to the Headteacher. Concerns relating to Safeguarding must be dealt with through the School's Safeguarding Policy and Procedures.
- All E-Safety complaints and incidents will be recorded in school, including any action taken.
- Any complaint concerning staff or pupil misuse of the internet must be reported to the headteacher immediately.

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

Monitoring and Reviewing

This policy is monitored by the Headteacher, who reports to the ASC about the effectiveness of the policy on request. It will be reviewed annually or appropriate to new legislation or to the needs of the school by the schools Computing lead. Any changes will be disseminated to staff and the ASC.

Reviewed annually

Useful links and Information for Staff

Teaching Online Safety in Schools

https://www.gov.uk/government/publications/teaching-online-safety-in-schools

Online Safety for SEND

https://www.childnet.com/resources/star-sen-toolkit

https://www.thinkuknow.co.uk/professionals/resources/

Gaming Advice

https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-games/

Online safety helpline

https://www.saferinternet.org.uk/our-helplines