NORWICH SCHOOL

e-Safety Policy

This policy is reviewed by the Head of IT and the Designated Safeguarding Lead (DSL) annually. This policy was last reviewed and agreed on Trinity 2023. It is due for review in Trinity 2024.

Confirmed by:

Terry Roberts	Head of IT	Trinity 2023
Nicky Fairweather	Principal Deputy Head & DSL	Trinity 2023

Version Control

The version control table should be updated each time:

- a **change** is made to an **agreed version** of a document; or
- a previously agreed document version is **reviewed with no changes** (i.e. at annual review no changes are required and the document continues to be live for the following year).

Use the following convention: version 1.0 (first version), version 2.0 (major change to version 1.0 and issued as a new version), version 2.1 (second version with minor change)

Version number	Date issued	Author / key contact	Change(s) summary • Minor changes can be authorised by a senior staff member and do not need formal approval. • Major revisions require approval through the confirming authority (typically a Committee)
1.0	Trinity 2022	Terry Roberts	
1.0	Trinity 2023		No changes

Contents page

Statement of intent

It is the duty of Norwich School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites
- email and instant messaging
- blogs
- social networking sites
- chat rooms
- music / video downloads
- gaming sites
- text messaging and picture messaging
- video calls
- podcasting
- online communities via games consoles
- mobile internet devices such as smart phones and tablets

This policy, supported by the IT Acceptable Use Agreement, applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users). It is implemented to protect the interests and safety of the whole school community and aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Health & Safety Policy
- Behaviour Support and Intervention Policy
- Anti-Bullying Policy
- IT Acceptable Use Agreements
- Social Media Policy
- Privacy Notice

- Bring Your Own Device – Staff, Visitors and Pupils

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Norwich School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

Purpose and Aims

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems and digital technology, both in and out of school. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. ‘Parents’ includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the IT Acceptable Use Agreement cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc), as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc), known as BYOD devices

Roles and responsibilities

The Governing Body

The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually.

Mr David Talbot has been appointed by the governing body to champion IT and e-Safety.

Head and the Senior Management Team

The Head is responsible for the safety of the members of the school community, and this includes responsibility for e-safety. The Head has delegated day-to-day responsibility to the Head of Digital Learning.

In particular, the role of the Head and the Senior Management team is to ensure that: staff, in particular the Head of Digital Learning, are adequately trained about e-safety; and staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection with the school.

Head of Digital Learning

The school's Head of Digital Learning is responsible to the Head for the day-to-day issues relating to e-safety. The Head of Digital Learning has responsibility for ensuring this policy is upheld by all members of the school community and works with IT staff to achieve this. They will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the Independent Schools Inspectorate (ISI), the Local Authority, Child Exploitation and Online Protection (CEOP), Childnet International and the Local Authority Safeguarding Children Board.

IT Staff

The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the Principal Deputy Head.

Teaching and support staff

All staff are required to agree to the IT Acceptable Use Agreement before accessing the school's systems.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

Pupils

Pupils are responsible for using the school IT systems in accordance with the IT Acceptable Use Agreement, and for letting staff know if they see IT systems being misused.

Parents

Norwich School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents and carers are responsible for endorsing the school's IT Acceptable Use Agreement.

Education and training

Staff: awareness and training

New staff receive information on Norwich School's e-Safety and IT Acceptable Use policies as part of their induction.

All staff receive information and training on e-safety issues in the form of INSET training and internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. [These behaviours are summarised in the IT Acceptable Use Agreement which must be signed and returned before use of technologies in school.] When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's Principal Deputy Head.

Pupils: e-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out within the PPD and Computer Science lessons programme, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their e-safety responsibilities and to look after their own online safety. From lower four pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Designated Safeguarding Lead and any member of staff at the school.

From middle five, pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc) through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-Bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the Designated Safeguarding Lead, School Nurse, Head of Digital Learning as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Parents

The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child(ren) when they use electronic equipment at home. The school therefore arranges annual discussion evenings for parents when an outside specialist advises about e-safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for schoolwork. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff are referred to the Bring Your Own Device (BYOD) Policy for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at Norwich School are permitted to bring in personal devices for their own use. Staff working in the Lower School or with Lower School pupils are not allowed to have their personal devices switched on during the working day. They may use such devices in the Lower School staffroom only.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents and under no circumstances may staff contact a pupil or parent using a personal telephone number, email address, social media, or other messaging system.

Pupils

If pupils bring in mobile devices to school, they will remain the responsibility of the child in case of loss or damage.

The school encourages the use of pupil owned devices as a teaching and learning tool and pupils are required to adhere to the Pupil BYOD Policy when using these devices for schoolwork. In particular, the BYOD Policy requires pupils to ensure that their use of tablets for schoolwork complies with this policy and the IT Acceptable Use Agreement and prohibits pupils from using tablets for non-school related activities during lesson time.

There are a number of school mobile technologies available for pupil use including laptops, tablets, cameras, etc during the school day. These devices are to be used in accordance with the IT Acceptable Use Agreement and e-Safety Policy.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the pupil’s Head of Section and SENCO to agree how the school can appropriately support such use. The SENCO will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

Use of internet and email

Staff

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with schoolwork or business whilst teaching/in front of pupils.

Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to Principal Deputy Head the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to IT Services Manager.

Any online communications must not either knowingly or recklessly

- place a child or young person at risk of harm, or cause actual harm
- bring Norwich School into disrepute

- breach confidentiality
- breach copyright
- breach data protection legislation
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
  - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
  - using social media to bully another individual; or
  - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should school pupils or parents be added as social network 'friends' or contacted through social media.

Any digital communication between staff and pupils or parents must be professional in tone and content. Under no circumstances may staff contact a pupil or parent using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all schoolwork, assignments / research / projects. Pupils should be aware that email communications through the school network and school email addresses are monitored.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for schoolwork / research purposes, pupils should contact IT Services Manager for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to the Principal Deputy Head.

The school expects pupils to think carefully before they post any information online or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the Principal Deputy Head. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Support and Intervention Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for schoolwork / research purposes, pupils should contact the IT Services Manager for assistance.

Data storage and processing

The school takes its compliance with Data Protection laws seriously. Please refer to the Data Protection Policy, Privacy Notice and the IT Acceptable Use Agreement for further details.

Staff and pupils are expected to save all data relating to their work to the school's central server / OneDrive cloud account.

Staff devices should be encrypted if any data or passwords are stored on them. No school owned date should be transferred outside of the school in an unencrypted format.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Assistant Bursar.

Password security

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

All pupils and members of staff should:

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

Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents of pupils in the Lower School are not permitted to take videos or digital images of school activities.

Parents of pupils in the Senior School may take videos and digital images of their children at some school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff are allowed to take digital / video images to support educational aims, but must follow this policy, the Privacy Notice and the Data Protection Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
Pupils must not take, use, share, publish or distribute images of others.

From time to time the school will publish photos and video of pupils and activities on the school website. Further information can be found in the Privacy Notice.

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs without the consent of the parents of, if appropriate, the pupils.

Misuse

Norwich School will not tolerate illegal activities or activities that are inappropriate in a school context and will report illegal activity to the police and/or the LSCB. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures in particular the Safeguarding and Child Protection Policy.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

Concerns and Complaints

As with all issues of safety at Norwich School, if a member of staff, a pupil or a parent has a concern or complaint relating to e-safety prompt action will be taken to deal with it.

Further information about how to raise a Concern or Complaint can be found in our Concerns and Complaints Policy.

Document control

Document title:	e-Safety Policy
Prepared by:	Terry Roberts
Authorised by:	Senior Management Team
Published location(s):	▪ Norwich School Website ▪ Norwich School Hub
Other internal policies / documents referenced:	▪ Anti-Bullying Policy ▪ Behaviour Support and Intervention Policy ▪ Bring Your Own Device – Staff, Visitors and Pupils ▪ Complaints Policy ▪ Health & Safety Policy ▪ IT Acceptable Use Agreements ▪ Privacy Notice ▪ Safeguarding and Child Protection Policy ▪ Social Media Policy ▪ Staff Code of Conduct
External documents referenced:	▪ Independent Schools Inspectorate (ISI) ▪ Child Exploitation and Online Protection (CEOP) ▪ Childnet International ▪ Local Authority Safeguarding Children Board