POLICY	**E-Safety**
STATUS/DATE OF THIS VERSION	**July 2021**
APPROVED BY	**Board of Trustees**
RATIFIED BY	**12th July 2022**
REVIEW	**July 2023**

This policy is operated by all the schools in Unity Education Trust (as listed below). **There may be sections that are specific to one school and these will be added by the school either as an annex or in place of yellow highlighted sections below.**

Any queries about the policy should be directed, in the first instance, to the Headteacher/Head of School:

- **Beeston Primary**
- **Garvestone Primary**
- **Grove House Infant**
- **Kings Park Infant**
- **Northgate High School and Dereham Sixth Form College**
- **The Pinetree School**
- **The Short Stay School for Norfolk**
- **Churchill Park**
- **Greyfriars Primary**
- **Highgate Infant School**
- **Kings Oak Infant School**
- **Wimbotsham and Stow Primary**
- **Magdalen Primary**
- **St Germans Primary**
- **Great Dunham Primary**

Teaching and Learning

The Internet is an essential element in the 21st century life. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The school Internet access is designed expressly for pupil use and includes filtering appropriate to the needs of the curriculum. Internet access will be planned to enrich and extend learning activities.

Access levels will be reviewed to reflect the curriculum requirements and age of pupils. Staff should guide pupils in online activities that will support the learning outcomes planned for the pupil's age and maturity. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Information System security

The Data and Systems Lead is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of Trust data and personal protection of our school communities very seriously. This means protecting the school networks, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the Trust's information systems and users will be reviewed regularly and virus protection software will be updated regularly. Some safeguards that the Trust takes to secure our computer systems are:

Making sure that unapproved software is not downloaded to any school computers.

Files held on the school networks will be regularly checked for viruses; Antivirus software is installed on all Trust PC's.

The use of user logins and passwords to access the school network will be enforced Portable media (USB, CDs, etc.) containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

For more information on data protection in school please refer to our GDPR Data Protection policy.

Core Principals of Internet Safety

In common with most technologies, internet use presents risks as well as benefits. Students could be placed in inappropriate and even dangerous situations without mediated internet access. To ensure responsible use and the safety of students the school's policy is built on the following five core principles:

1 Guided Educational Use
Internet use will be planned, task orientated and educational within a regulated and managed environment.

2 Risk Assessment
Both staff and students will be aware of the risks associated with internet use. Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school allowed. Staff and students will know what to do if they come across inappropriate material when using the internet.

3 Responsibility
Internet safety depends on staff, governors, advisors, parents and students themselves taking responsibility for use of the internet and associated technologies. The school will seek to balance education for responsible use, regulation and technical solutions to ensure student safety.

4 Regulation
The use of the internet, which brings with it the possibility of misuse, will be regulated. All staff and students are aware of the Trust ICT Acceptable Use Policy

5 Appropriate Strategies
Effective, monitored strategies will be in place to ensure responsible and safe internet use. The trust will work in partnership with Norfolk County Council's Children's Services, the Department for Education, parents and the Internet Service Provider to ensure systems to protect students are regularly reviewed and improved.

Internet Access

- Students

Parents/carers will be informed that students will be provided with monitored internet access and will be required to sign and return the ICT Acceptable Use Policy. acknowledging their understanding of the Trust's policy and internet and network use. The school will keep a record of all students who are granted internet access. The record will be monitored by the Data and Systems Lead.

- Staff, Governors and Community

Staff will be given access to the internet as part of their role within school. Governors and community users / visitors will be given access to a secure Wi-Fi connection when on site. Details of the Wi-Fi network can be obtained from the Headteacher. All staff must read and sign the Staff ICT Acceptable Use Policy before using any school ICT resource.

Emails

The Trust uses email internally for staff and students, and externally for contacting parents and other agencies, and is an essential part of Trust communication. It is also used to enhance the curriculum by providing immediate feedback on work, and requests for support where it is needed.

Staff and students must be aware that Trust/school email accounts must only be used for school related matters, i.e. for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

- Use of CC, BCC and Reply to All

Staff using Email should ensure that they are aware of the difference between CC and BCC and that caution is used when "replying to all" to ensure that information is not shared accidentally with those not relevant.

Staff are required to report to the school's GDPR co-ordinator immediately where an incorrect BCC/CC is used.

- School E-mail Accounts and Appropriate Use

Staff should only use official Trust/school-provided email accounts to communicate with students, parents or carers. Staff should not use official Trust/school provided email accounts for personal communications.

Emails sent from Trust/school accounts should be professionally and carefully written. Staff are representing the Trust at all times and should take this into account when entering into any email communications.

Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the Trust/school or from an external account. They should not attempt to deal with this themselves. Students will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

Under no circumstances should staff use personal email addresses to contact pupils or parents.

Social Networking and Personal Publishing

The school will block access to social networking sites, unless their unblocking is specifically requested by a member of staff to meet clear educational objectives. Pupils and staff will be advised never to give out personal details of any kind which

may identify themselves or others and /or their location. Examples would include real names, addresses, full names of friends, specific interests etc.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary pupils and requires close monitoring with older pupils. Pupils will be taught how to use social networks in a safe and responsible way, including how to ensure their safety on social networks, how to find help and how to identify some of the dangers of social networking.

All users should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. If staff become aware of any inappropriate or unsafe contact on social networks by a pupil, they will contact the pupil's parents/guardians and CEOPs where appropriate. Staff are **advised not** to be 'friends' with students and ex-students on social networking media such as Facebook.

Mobile Phones
Whilst we acknowledge that mobile phones are part of modern life, they distract from learning and can be misused in terms of social media linked to cyberbullying.

Pupils can choose to bring mobile phones or other electronic devices into school but will be responsible for their safekeeping: the school and Trust will not be responsible should they go missing or be stolen. Students should not use or have their mobile phone or other electronic devices (including but not limited to speakers, earphones, and smart watches) switched on or visible whilst on school site unless permitted in lessons if expressly linked to the learning and authorised by the Teacher. Outside of this, students seen with or using electronic devices will have them confiscated and can collect them at the end of the day. All confiscated items will be held securely. For NGHS-a subsequent confiscation will require collection by a parent/guardian – this will be logged by administration staff. Failure to hand over any item will result in the pupil being placed in internal exclusion for the remainder of the school day, parents contacted, and further restriction placed on the offending item.
For Specialist- contact will be made with the parents reminding them of the requirements and to encourage advising their child of potential educational consequences.

If a student needs to contact their parents/carers they will be allowed to use a school phone. If parents/carers need to contact their child urgently they should phone the school office and a message will be relayed promptly.

The Trust accepts no responsibility for theft, loss or damage relating to phones/devices including those handed in/confiscated.

Under no circumstances should staff use their own personal devices to contact students or parents either in or out of school time unless in an emergency. **Staff are not permitted to take photos or videos of students on their own devices**. If photos or videos are being taken as part of the school curriculum or in a professional

capacity, the school equipment must be used and ensure photo consent has been provided. The Trust expects staff to lead by example. Personal mobile phones should be switched off or on 'silent', and kept out of sight, during school hours. Work mobiles can be visible.

With the authorisation of the local Headteacher, some teams may use their personal mobile phones to make calls, texts or WhatsApp group in order to ensure effective communication or to ensure pupil or staff safety. Alternatively, communication radios are available, subject to site.

Any breach of policy may result in disciplinary action against that member of staff.

- Students

The sending of abusive or inappropriate text messages is forbidden and may be illegal. The inclusion of inappropriate language or images within text messages is difficult for staff to detect. Students will be reminded that such use is both inappropriate and conflicts with school policy. Abusive messages will be dealt with under the school Anti-Bullying Policy; this includes 'videoing' of incidents.

- Staff

Staff will be issued with a school phone where required or the school's communication technology will need to be used. **No contact with students or their families will be made by way of personal devices and staff must use school owned equipment.**

Publishing Students' Images and Work

Photographs that include students will be selected carefully and will not enable individual students to be clearly recognised unless express permission has been given by an adult with parental responsibility. This permission is requested when each student joins the school and is recorded onto the school management information system. Full names will not be used in association with photographs.

Filtering and Monitoring

The school uses regularly updated and dedicated systems to filter internet content and monitor all student user activity on the network. Email messages are monitored and all suspicious items are alerted to designated staff.

Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The Data and System Lead, in liaison with the Directorate Leads, will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The Trust keeps up-to-date with new

technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Cyber Bullying

Cyber bullying is a form of harassment using information and communications technology (ICT), particularly; mobile phones, social media and internet, with the purpose of trying to deliberately upset and intimidate someone else. It is a "method" rather than a "type" of bullying and includes bullying via text message, instant messaging services, social network sites, email, images and videos posted on the internet or spread by mobile phone.

- Students, Parents and Carers

Parents and carers need to be aware that many children have been involved in cyberbullying in some way, either as a victim, perpetrator, or bystander. By its very nature, cyberbullying tends to involve a number of online bystanders and can quickly spiral out of control. Children and young people who bully others online do not need to be physically stronger and their methods can often be hidden and subtle.

If students or parents / carers of students believe they are being bullied online by another student, they should report this to their Teacher/DSL who will investigate the incident and use sanctions set out in the behaviour policy to deal with any perpetrators. Where possible, screenshots and evidence of any online activity should be recorded.

Parents/ carers should report any instances of cyber bulling where it is carried out by an external perpetrator, directly to the Police or via CEOPs.

- Staff

The school is committed to protecting staff against cyber-bullying and online harassment and take the complaints of staff members as seriously as the complaints of students and parents. Any member of staff who believes they are being bullied or harassed online should report this to the senior leadership team at the school who will investigate the incident. Where possible, screenshots and evidence of any online activity should be recorded.

Staff should report any instances of cyber bulling, where it is carried out by an external perpetrator, directly to the Police or via CEOPs.

Protecting Personal Data

UET believes that protecting the privacy of our staff, Governors and students and regulating their safety through data management, control and evaluation is vital. The Trust/schools collect personal data from students, parents, governors and staff and process it in order to support teaching and learning, monitor and report on student

and teacher progress, provide information to Government and to strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as necessary. Assessment results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of provisions and evaluate the wellbeing and academic progression of our school community to ensure that we are doing all we can to support both staff and students.

We have appointed a DPO in line with the GDPR requirement and provide privacy notices to all staff, students, and contractors to advise of the processing of their data.

Ethnicity and Diversity

The Unity Education Trust is committed to equal opportunities for all, regardless of age, race, religion, gender, sexual orientation, class or disability. The Trust recognises that it has a statutory duty under the Equality Act 2010 to pay 'due regard' to the following when exercising public functions:

- Eliminate discrimination, harassment and victimisation and other prohibited conduct
- Advance equality of opportunity
- Foster good community relations

We will not treat anyone less favourably than any other, on the grounds of any protected characteristic, except when such treatment is within the law, and determined by lawful requirement