| | |
|---|---|
| **POLICY** | **E-Safety Policy** |
| **STATUS/DATE OF THIS VERSION** | **July 2023** |
| **APPROVED BY** | **Board of Trustees** |
| **RATIFIED BY** | **Board of Trustees – June 2023** |
| **REVIEW** | **July 2024** |

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**

# 1 Aims

Unity Education Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

# 2 The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as child or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

# 3 Core Principals of Online Safety

Students could be placed in inappropriate and even dangerous situations without mediated internet access. To ensure responsible use and the safety of students the Trust's policy for addressing the categories of risk 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.

# 4 Roles and responsibilities

## 4.1 The Trust board

The Trust board has overall responsibility for monitoring this policy for its implementation. The Directorate Leads will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs.

All Trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on the Trust ICT Acceptable Use Policy.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

## 4.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

## 4.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and alternate DSLSs are set out in our school's child protection and safeguarding policies, on posters, as well as in relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing board.

This list is not intended to be exhaustive.

## 4.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the Trust's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately.
- Updating and delivering staff training on online safety.
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

## 4.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the Trust ICT Acceptable Use Policy and ensuring that pupils follow the Trust's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

## 4.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the Trust ICT Acceptable Use Policy

Parents can seek further guidance on keeping children safe online from organisations, such as: UK Safer Internet Centre, Childnet, CEOP.

### 4.7 Visitors and members of the community

Visitors and members of the community who use the Trust's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to read and agree to Trust ICT Acceptable Use Policy.

## 5 Teaching and Learning

The Internet is an essential element in the 21st century life. The Trust has a duty to provide students with quality Internet access and system security 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.

### 5.1 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 'Trust ICT Acceptable Use Policy – Student'. 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 Trust ICT Manager.

**Staff, Governors and Trustees**

Staff will be given access to the internet as part of their role within school. All staff must read and sign the 'Trust ICT Acceptable Use Policy – Staff' before using any school ICT resource.

**Visitors and Community**

School visitors and community users will be entitled to have access to a secure guest Wi-Fi connection when on site. Details of the guest Wi-Fi network can be obtained from the Trust ICT Manager. All users of the guest Wi-Fi must read and sign the 'Guest WiFi Disclaimer' before access is permitted.

### 5.2 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.

### 5.3 Information System security

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.

The Trust ICT Manager 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.
- Restricts the use of personal portable media devices (USB, external hard drives, etc).

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

## 5.4 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.

For more information on the use of email please refer to our Communications and Social Media Policy.

## 5.5 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.

For more information on Social Networking please refer to our Communications and Social Media Policy.

### 5.6 Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The Trust ICT Manager, 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.

### 5.7 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.

## 6 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.

# 7 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.
- For some settings there may be a local arrangement in place, where this is the case, this will be outlined by the school.

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**. **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.**

Any staff provided with a school phone will be required to sign and adhere to the Trust's mobile phone agreement.