E-Safety Policy

Contents

1. **Introduction**
2. **Scope of this policy**
3. **Roles and responsibilities**
    a. The Governing body
    b. Head of School and Senior Leadership Team
    c. ICT Co-ordinator
    d. One Education – ICT technicians
    e. Staff and volunteers
    f. Pupils
    g. Parents and carers
4. **Education and Training**
    a. Staff awareness and training
    b. Pupils: E-safety in the curriculum
    c. Parents and carers
5. **Policy statements**
    a. Use of personal devices
    b. Use of internet and email
    c. Password security
    d. Safe use of digital and video images
    e. Misuse
    f. Complaints

Introduction

At the Schools of the Children of Success Schools Trust we encourage student engagement with information and communication technology (ICT) as we believe that it enables them to learn, communicate and explore the world in new ways.

It is the duty of the Trust to ensure that every pupil in its care is safe, and this applies equally as regards the digital world and the real world. IT and online communications can provide valuable opportunities for learning, but can also pose significant risks to young people. Our pupils are therefore taught about the risks they face online and how to limit them; these risks include, but are not limited to, fraud, malicious software, the risk of identity theft, bullying, grooming, stalking, abusive behaviours (e.g. trolling) 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 and conferencing, podcasting, online communities via games consoles, IoT devices (e.g. Amazon Echo) and mobile devices (e.g. smart phones and tablets).

This policy, supported by the Acceptable Use Policy, is implemented to protect the interests and safety of the whole school community. It 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, Code of Conduct for Staff, Health and Safety Policy, Behaviour, Rewards and Sanctions Policy, Anti-Bullying Policy, Acceptable Use Policy, Social Media and Online Activity Policy, Data Protection Policy, Bring Your Own Device Policies and PSHE scheme of work.

Whilst recognising the potential benefits of the above innovations, it is important to remember that these internet technologies are not consistently policed. All users therefore need to be aware of the range of risks associated with them and the potential for a negative impact on mental health and well-being.

At the Schools of the Trust, we understand our responsibility to educate our pupils on E-Safety issues. We aim to equip pupils with the strategies and critical thinking skills needed to enable them to remain safe and within the law when using the internet and related technologies. 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.

Scope of this Policy

This policy applies to all members of the School community who have access to the School's IT systems, including staff, IT technician, pupils, volunteers, parents and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Visitors' includes anyone else who comes to the School, including occasional volunteers.

Both this policy and the Acceptable Use Policy 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 any personal devices brought onto school premises.

Roles and responsibilities

1. The Governing Body

The governing body of the School is responsible for the approval of this policy and for reviewing its effectiveness. It will review this policy at least every three years.

The nominated governor for safeguarding takes responsibility for ensuring that the E-Safety Policy is implemented.

2. The Head of School and the Senior Leadership Team

The Head of School is responsible for the safety of the members of the School community, and this includes responsibility for E-Safety and for ensuring this policy is upheld by all members of the School community. The Head of School has delegated day-to-day responsibility to the Designated Safeguarding Lead and curriculum support from the ICT Coordinator.

In particular, the role of the Head of School and the Senior Leadership team is to ensure that:

- staff, in particular the ICT Coordinator, 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 to the School.

Designated Safeguarding Lead

The Designated Safeguarding Lead is responsible to the Head of School for addressing issues in relation to pupils where there might be cyber bullying, working with the ICT Co-ordinator to involve parents and carers in information sharing regarding E-safety.

3. ICT Coordinator

The ICT Coordinator is responsible for the e-safety curriculum, ensuring it is delivered, kept up to date and that staff are adequately trained to deliver it.

The post-holder will keep up to date on current e-Safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board. Using this information they are responsible for increasing awareness of e-safety issues with parents (including updating the e-safety page of the school website, pupils and staff.

The post holder is responsible for informing the SLT of any e-safety issues that arise.

4. Computer Services staff – One Education

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 and its data. They provide appropriate access to, and monitor the use of, the internet and the possibility to access and monitor emails; they maintain content filters and report inappropriate usage to the Head of School.

5. Staff and volunteers

Anyone accessing the School's IT infrastructure is required to abide by the Acceptable Use Policy.

All staff working with pupils are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. 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 on a daily basis.

Staff have a responsibility to record and report any incidents or concerns relating to E-Safety using the Child Protection Online Monitoring System (CPOMS).

6. Pupils

Pupils are required to abide by the Acceptable Use Policy when accessing the School's IT infrastructure, and must let staff know if they see IT systems being misused.

7. Parents and carers

Parents and carers are responsible for endorsing the School's Acceptable Use Policy, and for promoting E-Safety, both in and outside of school. This will be encouraged through dialogue regarding the E-safety issues.

Education and training

1. Staff: awareness and training

New staff receive information on the School's E-Safety and Acceptable Use Policies as part of their induction.

Staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety. They also receive, as and when appropriate, additional guidance and training on E-Safety issues in briefings and CPD sessions.

2. Pupils: E-Safety in the curriculum

IT and online resources are used across the curriculum. As part of the ICT curriculum, the children complete a Computer passport which includes information regarding the Acceptable Use Policy and E-Safety guidance. Aspects of E-Safety are also covered in PSHE lessons and assemblies, and also informally, when opportunities arise. We review and modify our provision in the light of changing needs.

As a Rights Respecting School, our ethos and programme reinforces many aspects of E-safety.

At age-appropriate levels, pupils are taught about their E-Safety responsibilities, and to look after their own online safety. From an appropriate age, pupils are formally/informally taught about recognising online sexual exploitation, stalking and grooming, radicalisation and hatred, the risks, and of their duty to report any such instances they or their peers come across. Pupils are made aware that they can report concerns to the DSL or any other member of staff at the School.

Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

Each pupil has a computing passport which they complete during the year part of which is clear about acceptable use and other issues relating to e-safety.

Pupils are made aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues. (The School's Anti-bullying Policy describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying). Pupils should approach any member of staff, as well as parents and their peers, for advice or help if they experience problems when using the internet and related technologies.

3. Parents/carers

The School seeks to work closely with parents and carers 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 carers may feel equipped to protect their child/children when they use electronic equipment at home. The School therefore from time to time arranges e-safety events for parents to provide advice on E-Safety and the practical steps parents can take to minimise the potential dangers to their son(s).

For further guidance and access to E-Safety resources, visit www.childnet.com.

Policy Statements

1. 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. (For further details of password security, see below.) When the device is not being used it should be locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff are permitted to bring in personal devices for their own use such as mobile phones but usage must be in accordance with the Code of Conduct for Staff and the acceptable use policy.

Pupils

The pupils are not permitted to bring into school mobile devices. If a child brings a mobile phone it must be handed into reception or the front desk, at the start of the school day. The School does not accept any responsibility for loss or damage and the phones are brought in at their own risk.

The School recognises that mobile devices are sometimes used by pupils 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, this will be discussed by the SEND department with the pupil's parents or carers.

Once agreement is reached, the SEND Department will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

2. Use of internet and email

Staff

Staff must at all times act in accordance with guidance in the Code of Conduct for Staff and Acceptable use policy.

All digital communication between staff and pupils must take place using class school accounts. Staff are expressly forbidden from having contact with pupils via private email or social media accounts.

The School has taken all reasonable steps to ensure that the School network is safe and secure. Staff should be aware that all activity on the School's network, including email communication via staff email addresses, can be monitored.

Communication between staff and pupils or parents/carers on other media platforms, including 2Simple, Class Dojo and Twitter must be professional in tone and content.

When using school systems, staff should immediately report to the ICT Coordinator or DSL any online material or email communication which makes them feel uncomfortable, or is offensive, discriminatory, threatening or bullying in nature. They must not respond to any such communication.

Staff must remain alert to the risk of fraudulent emails. They should report emails they suspect to be fraudulent to the ICT Coordinator, DSL or One Education technician.

Pupils

All pupils are issued with usernames for use on our network. Access is via a personal login, which is password protected. Pupils should be aware that computer access to the internet is 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.

Pupils must not seek to contact staff via private email or social media accounts.

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 a member of staff.

The School expects pupils to think carefully before they post any information online, or re-post 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 their class teacher or other member of staff. The deliberate accessing of inappropriate material by a pupil will lead to the incident being recorded on their file and will be dealt with under the School's Behaviour

Policy. Pupils should be aware that all internet usage via the School's systems, including its Wi-Fi network, is monitored.

Certain websites are automatically blocked by the School's filtering system.

4. Password security

Staff have individual school network logins, and personal storage folders on the server. Pupils have class logins. Staff and pupils are regularly reminded (every 180 days) of the need for password security.

All staff and pupils should:

- use a strong, unique password consisting of at least 8 characters. This should include a mixture of capital and lower case letters, numerals and special characters. It must not include a group of three characters from the username. As a matter of good practice it should be changed every 6 months.
- **never share their passwords.**

5. 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/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying, 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 their creation, use, sharing, publication and distribution. In particular, they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents/carers are permitted to take videos and digital images of their own children at school events for their own personal use, provided that they have the permission of the member of staff responsible for the event. To respect everyone's privacy and, in some cases, protection, these images must not be published (e.g. on blogs or social networking sites) 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 and volunteers are allowed to take digital/video images to support educational aims, but must follow the School’s acceptable use policy and the sharing, distribution and publication of those images is not permitted outside the school.

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.

Photographs published on the School website, or displayed elsewhere, which include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. When

photographs are to be published accompanied by the full names of pupils, permission from parents/carers will be obtained.

6. Misuse

The Children of Success Schools Trust 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 Manchester Safeguarding Children Board. 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 Child Exploitation and Online Protection Centre.

Incidents of misuse or suspected misuse will be dealt with by staff in accordance with the School's policies and procedures. Any misuse by parents against staff or pupils will be dealt with and reported to the police.

In accordance with the Behaviour Policy, the school will impose one of a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil.

Complaints

As with all issues of safety at Haveley Hey, The Willows or The Bridge, if a member of staff, a pupil or a parent/carer has a complaint or concern relating to E-Safety, prompt action will be taken to deal with it. Complaints should be addressed to the School's DSL. Please see the Complaints Policy for further information.