OLDHAM HULME GRAMMAR SCHOOL

E SAFETY POLICY

This policy is applicable from EYFS through to year 13

Introduction and Overview

E-Safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- e-Safety concerns safeguarding children and young people in the digital world.
- e-Safety emphasises learning to understand and use new technologies in a positive way.
- e-Safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
- e-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

The internet is an unmanaged, open communications channel. The World Wide Web, email, blogs and social networks all transmit information using the internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the internet make it an invaluable resource used by millions of people every day.

Some of the material on the internet is published for an adult audience and can include violent and adult content. Information on weapons, crime, extremism, self harm, risky behaviours and racism may also be unsuitable for children and young people to access. Pupils need to develop critical skills to evaluate online material and learn that publishing personal information could compromise their security and that of others. Schools have a duty of care to enable pupils to use online systems safely.

This e-safety policy operates in conjunction with other school policies including Behaviour, Safeguarding and Anti-Bullying.

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by our Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where appropriate, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Oldham Hulme Grammar School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Oldham Hulme Grammar School.
- 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.

- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- 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.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyberbullying in all forms
- identity theft
- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and wellbeing (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

2. Education and Curriculum

Pupil e-Safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computer science curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
- to STOP and THINK before they CLICK;
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;

- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- from KS2 to understand why and how some people will 'groom' young people for sexual reasons;
- to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

Staff and governor training

Regular whole school staff training will be held to appraise staff, particularly those with pastoral roles, of current issues and developments in students' online behaviour. Pastoral staff will be encouraged to attend any relevant external training and the school will aim to have at least one 'CEOP ambassador' in each section. Pastoral staff will discuss any issues arising at regular pastoral meetings, and will pass on any relevant information to form tutors either within form tutors' meetings or an individual basis.

The DSL and DDSLs will liaise with our local area designated officer to maintain awareness of the local context and any significant issues in the local community.

Governors will be invited to attend any staff training.

Induction

Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the eSafety policy and the school's Acceptable Use Policies.

Parent awareness and training

E-safety will form part of our introductory evening for all parents of year 7 pupils.

E-safety events will be held during the school year and parents will be invited to participate. Literature relating to safety will be available at parents' evenings. Printed and online e-safety information will be made available to all parents.

Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying
- Staff are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and handheld devices.

- students/pupils should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- parents/carers should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions.
- we use Securly to monitor work being completed by pupils and maintain a record of this.
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (eg the local authority, CEOP, police) in dealing with e-safety issues
- monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school.
- parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This school:

- Has educational, filtered, secure broadband connectivity.
- Uses filtering systems which block sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all students have signed a responsible email and internet use consent form and understands that they must report any concerns;
- Requires staff to preview websites before use [where not previously viewed or cached]. Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg Google Safe Search , …..
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the system administrator(s) who logs or escalates as appropriate referring to the relevant senior leader;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – CEOP or the Police.

Network management

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique username and password.
- Ensures staff access to the school's management information system is controlled through a separate password for data security purposes;
- Ensures all pupils have their own unique username and password which gives them access to the Internet.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used solely to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.

E-mail

This school

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- Knows that spam, phishing and virus attachments can make emails dangerous.

Pupils:

- Pupils are introduced to, and use email as part of the ICT/Computing scheme of work.
- Pupils are taught about the safety of using email both in school and at home i.e. they are taught:
- that an e-mail is a form of publishing where the message should be clear, short and concise;
- they must not reveal private details of themselves or others in email, such as address, telephone number, etc;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- that they should think carefully before sending any attachments;
- that they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening emails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them;
- Pupils sign the school Agreement Use Agreement Form to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with.

Staff:

- May use email to communicate with parents but when doing so will ensure professional language is used and, where this is potentially contentious, will cc their line manager or head or department.

- Staff know that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style'.
- See 'Staff email protocol' for further guidance.
- Should always remember to STOP and THINK before they CLICK;

School website

- The Principal takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained; This responsibility is delegated on a day to day basis to; Marketing Manager/Deputy Principal/ Principal's PA.
- We expect teachers using school approved blogs or twitter accounts to password protect them and use appropriate professional language.

Social networking

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school.*
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's & parent's or visitor's own risk. The School accepts no responsibility for the loss, theft or damage of any phone, laptop or handheld device brought into school.
- Pupil mobile phones which are brought into school must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. Staff members should not use their mobile phones during lesson times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the principal or deputy principals. Such authorised use is to be monitored and recorded.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or handheld devices may be searched at any time as part of routine monitoring.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff. They should be switched off or silent at all times.
- The Bluetooth or similar function of a mobile phone should not be used to send images or files to other mobile phones.

Pupils' use of personal devices

- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff are advised not to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. (Except in the event of an emergency)

Digital images and video

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Appendices:

Acceptable use agreement
Staff email protocol

Other relevant documents available

Oldham Hulme Grammar School – Staff Handbook
Staff Code of Conduct
Physical Intervention Policy

E Safety policy reviewed: November 2020

Next Review Due: November 2023