Academies Trust

8th Floor, Angel Square,
Manchester, M60 0AG

Online Safety Policy

Approved by Governing body on
Applicable from

This School is committed to safeguarding and promoting the welfare of its children and young people and expects all staff, agency staff, volunteers and visitors to share the same commitment

What is an Online Safety Policy?

- The school online safety policy aims to create an environment where pupils, staff, parents, governors and the wider school community work together to inform each other of ways to use the Internet responsibly, safely and positively.
- Internet technology helps pupils learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The online safety policy encourages appropriate and safe conduct and behaviour when achieving this.
- Pupils, staff and all other users of school related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour.
- These agreements and their implementation will promote positive behaviour which can transfer directly into each pupil’s adult life and prepare them for experiences and expectations in the workplace. The policy is not designed to be a blacklist of prohibited activities, but instead a list of areas to discuss, teach and inform, in order to develop positive behaviour and knowledge leading to a safer Internet usage and year on year improvement and measurable impact on online. It is intended that the positive effects of the policy will be seen online and offline; in school and at home; and ultimately beyond school and into the workplace.

Date: March 2020

Table of Contents

Introduction & Ethos

The school Online Policy aims to create an environment where pupils, staff, parents, governors and the wider school community work together to inform each other of ways to use the Internet responsibly, safely and positively.

Internet technology helps pupils learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The Online Policy encourages appropriate and safe conduct and behaviour when achieving this. It is underpinned by the school's Acceptable Use Policy.

The school will make reasonable use of relevant legislation and guidelines to inform positive behaviour regarding ICT and Internet usage both on and off the school site. This will include imposing sanctions for inappropriate behaviour in line with the regulation of student behaviour under the *Education and Inspections Act 2006*.

Pupils, staff and all other users of school-related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour. It is intended that the positive effects of the policy will be seen online and offline, in school and at home and, ultimately, beyond school and into the workplace.

The online policy and Acceptable Use Policy will be reviewed at, or prior to, the start of each academic year and promptly in the following instances:

- Serious and/or frequent breaches of the Acceptable Internet Use Policy or in the light of online incidents.
- New guidance by government/local authority/safeguarding authorities.
- Significant changes in technology as used by the school or pupils in the wider community.
- Online incidents in the community or local schools which might impact on the school community.
- Advice from the police and/or local safeguarding children partners.

Who This Policy Applies To

The school Online Policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider school community who use, have access to, or maintain school and school-related Internet, computer systems and mobile technologies internally and externally.

‘In loco parentis’ provision under the Children Act 1989 also allows the school to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils and removing inappropriate content.

Scope

This online policy covers the use of:

- School-based ICT systems and equipment
- School-based Intranet and networking
- School-related external Internet, including but not exclusively, extranet, e-learning platforms, blogs and social media websites
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing
- School ICT equipment off-site, for example, staff laptops, digital cameras, mobile phones, tablets
- Pupil and staff personal ICT equipment when used in school and which makes use of school networking, file-serving or Internet facilities
- Tablets, mobile phones, devices and laptops when used on the school site

Ofsted Context

Online safety is covered by the current Ofsted inspection framework.

When preparing a judgement, behaviours and attitudes will be considered and in particular, on the subject of online, inspectors will be looking for factors including "an environment in which pupils feel safe, and in which bullying, discrimination and peer-on-peer abuse – online or offline– are not accepted and are dealt with quickly, consistently and effectively whenever they occur".

Online safety will also be considered under personal development. Inspectors will be looking for evidence that pupils are able to recognise risks to their well-being both online and offline, for example, CSE, extremism etc and are aware of the support available to them.

In the context of safeguarding, schools should act in the best interest of the pupils to protect them both online and offline. Schools should be able to:

- Identify pupils at risk, for example through grooming
- Help pupils in need and refer to experts is necessary
- Manage safe recruitment and allegations about adults who may be a risk to pupils

Roles & Responsibilities

1) Principal and Academy Leadership Team

The school senior leadership is responsible for:

- Determining, evaluating and reviewing online policies to encompass teaching and learning, use of school IT equipment and facilities by pupils, staff and visitors.
- Agreeing criteria for the acceptable use by pupils, school staff and governors of Internet capable equipment for school-related purposes or in situations which will impact on the reputation of the school, and/or on school premises.

They will ensure that:

- There is a cycle of evaluation and review based on new initiatives and partnership discussion with stakeholders and outside organisations, technological and Internet developments, current government guidance and school-related online incidents.
- Good practice is implemented within the teaching curriculum and wider pastoral curriculum.
- Inset development is identified and provided for staff and governors and guidance provided to parents, pupils and local partnerships.
- Management is encouraged to be aspirational and innovative in developing strategies for, and a calendar of, online provision which will deliver measurable success and clearly state online targets with success criteria on the school development plan.

2) Online officer or coordinator

The school has a designated online officer Katharine Needham who reports to the ALT and governors and coordinates online provision across the school and wider school community.

- The online coordinator is responsible for online issues on a day-to-day basis including:
- Liaising with LA/Trust contacts, filtering and website providers and school ICT support.
- Maintaining a log of submitted online reports and incidents.
- Auditing and assessing inset requirements for staff, support staff and governor online safety training, and ensuring that all staff are aware of their responsibilities and the school's online safety procedures.
- Monitoring Internet usage by pupils and staff, including on school machines, such as laptops, used off-site.
- Promoting best practice online within the wider school community, including providing and being a source of information for parents and partner stakeholders.Along with IT

support and the computing coordinator, risk assessing new technologies, services or software.

3) Governors

The school has appointed Julian Gorton *as having* responsibility for online safety.

This governor will:

- Provide and evidence a link between the school, governors and parents.
- Liaise with the online officer/coordinator with regard to reports on online effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community. Complete an audit of Governor IT competence, relevant outside experience and qualifications to identify training needs and create a schedule and development plan.

4) ICT support staff & external contractors

Internal ICT support staff and technicians are responsible for:

- Maintaining the school's networking, IT infrastructure and hardware.
- Keeping up to date with current thinking and trends in IT security.
- Ensuring that the school system, particularly file-sharing and access to the Internet, is secure.
- Taking all reasonable steps to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.
- Maintaining and enforcing the school's password policy and monitoring and maintaining the Internet filtering.
- Ensuring external contractors, such as VLE providers, website designers/hosts/maintenance contractors, are made aware of, and comply with, the school's online policy.
- Completing DBS checks where contractors have access to sensitive school information and material covered by the Data Protection Act.

Where IT is outsourced, for example connectivity, maintenance, cloud-based services, website and email provision, filtering and anti-virus, the school needs to ensure that they comply with DfE guidance and that a Service Level Agreement (SLA) is in place to provide school standard provision and support.

5) Teaching and teaching support staff

Teaching and teaching support staff need to:

Ensure that they are aware of the current school policy, practices and associated procedures for reporting online incidents.
Read, understand and sign the Acceptable Use Policies relevant to Internet and computer use in school.
Follow the school's social media policy, which includes external off-site use, personal use (mindful of not bringing the school into disrepute), possible contractual obligations, and conduct on Internet school messaging or communication platforms, for example email, VLE messages and forums and the school website.
Rigorously monitor pupil Internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the school site.
Promote best practice regarding avoiding copyright infringement and plagiarism.
Be aware of online propaganda and help pupils with critical evaluation of online materials.
Internet usage and suggested websites should be pre-vetted and documented in lesson planning.
The school does not allow students to use their own devices in the academy.

Designated safeguarding lead

Every school and college should have a designated safeguarding leader (DSL) who is also a member of the school leadership team. This person will help staff carry out their safeguarding duties and liaise with third parties as required. The DSL should undergo appropriate training (for example, that provided by CEOP/ThinkUKnow), but this training should be supplemented regularly with further training, briefings, bulletins etc to help them keep up with developments.

Lauren Whyte is the designated safeguarding lead. The DSL is trained in specific online issues to enable them to decide which online incidents are required to be reported to CEOP, local Police, LADO, local safeguarding partners, Trust CEO, social services and parents/guardians; and also to determine whether the information from such an incident should be restricted to nominated members of the leadership team.

The DSL acts 'in loco parentis' and will liaise with websites and social media platforms such as Twitter and Facebook to remove instances of illegal material or cyber bullying.

6) Pupils

Pupils are required to:

- Use school Internet and computer systems in agreement with the terms specified in the school Acceptable Use Policies.
- Understand that the policies also cover the use of personal items such as phones and their Internet use out of school on social networking sites such as Instagram if it impacts on the school and/or its staff and pupils in terms of cyber bullying, reputation, YPSI or illegal activities.
- Be aware of how to report online incidents in school, and how to use external reporting facilities, such as the Click CEOP button or Childline number.

7) Parents & carers

Parents and carers are asked to support the school's stance on promoting good Internet behaviour and responsible use of IT equipment and mobile technologies both at school and at home.

The school expects parents and guardians to sign the school's Acceptable Use Policies, indicating agreement regarding their child's use and also their own use with regard to parental access to school systems such as extranets, websites, forums, social media, online reporting arrangement, questionnaires and the VLE.

The school will provide opportunities to educate parents on online.

8) Other users:

School visitors, wider school community stakeholders and external contractors should be expected to agree to a visitor's AUP document or a tailored AUP document specific to their level of access and usage.

External users with significant access to school systems which include sensitive information or information held securely under the General Data Protection Regulations should be DBS checked. This includes external contractors who might maintain the school domain name and web hosting – which would facilitate access to cloud file storage, website documents and email.

Online in Practice

The school will ensure that:

- School computer systems are fit for purpose and customised to ensure online while meeting
- teaching and learning requirements.
- It is possible to trace every login, data transaction, or other activity to a particular user.
- Servers, network switches, cloud-based systems, hubs, Cat5 or Fibre Optic cabling, wireless transmitters, bridges, access points and other physical architecture should be secured to prevent unauthorised or untraceable network access.
- Risk assessments will be made of any new equipment, technologies or systems.
- Regular audits of systems are carried out.
- The school's Internet service is provided by a fully accredited ISP.
- Filtering and monitoring is in place and any filtering incidents are examined to prevent a re-occurrence.
- The school has in place a password policy that is fit for purpose with pupils and staff encouraged to change passwords regularly.
- The school has protocols in place to meet the requirements of GDPR as defined by the Information Commissioner's Office.
- When disposing of equipment, the school ensures all data is wiped irretrievably.
- Policies are in place around the taking and sharing of images of children.
- The school will make it clear to pupils and staff which online and network activities are appropriate and which are not.

Online Education Programme

The school’s online education is delivered through PSHCE and ICT

The online education programme is delivered by teachers of PSHCE and ICT

Dealing with Online Incidents

Typical online incidents perpetrated by pupils, staff, parents, governors, contractors and others include:

- Finding illegal material on the network which could raise a child protection issue.
- Going on the Internet during lesson time for reasons not related to the lesson.
- Bypassing the school’s filtering system.
- Viewing pornographic material.
- Using a mobile phone or other digital device in a lesson.
- Using social media or email during a lesson.
- Cyber bullying.
- Writing malicious comments about the school or bringing the school name into disrepute (whether in school time or not).
- Sharing usernames and passwords.
- Deleting someone else’s work or unauthorised deletion of school files.

- Trying to hack or hacking into another person’s account, school databases, school website, school emails or online fraud using the school network.
- Uploading or downloading files using the school network.
- Copyright infringement of text, software or media.

The school’s approach to dealing with an incident and applying sanctions aims to demonstrate the correlation between procedures and sanctions for pupils and procedures and sanctions for staff.

The reporting process and sanctions will depend on:

- Whether an illegal act has taken place
- Whether there is a safeguarding issue (in which case we will follow the guidelines in our Safeguarding Policy)
- The nature and severity of the incident
- Whether the person has previously had sanctions for a similar incident

Note that under The Education and Inspections Act 2006 headteachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site. Also, staff can confiscate mobile phones if they cause a disturbance in class in breach of the school Behaviour Policy.

These general principles apply in dealing with an incident:

- Evidence should be collected and preserved – this may involve assistance from the school network manager, IT support or external IT contractor.
- Incident reports will be completed and submitted to Katharine Needham. Depending on the nature of the incident it should also be logged on CPOMS / report year managers.
- Appropriate disciplinary action/sanctions will be taken following the school’s procedures.
- Parents/carers may be informed.
- The police and/or other relevant agencies will be notified in certain circumstances, including:
    - if an indecent image has been taken
    - in the case of cyber bullying
    - An incident of hacking or online fraud
- Offending content will be removed if possible.
- A review of security will be carried out where relevant.

If a website is hosted in the USA, or operates under US law, then the *Digital Millennium Copyright Act* will apply for copyright infringement. This is very useful when seeking to remove photographs and other material which has been copied on to a site such as Facebook and Twitter.

Useful links

Ofsted:

www.gov.uk/government/publications/school-inspection-handbook-eif

DfE:

www.gov.uk/government/groups/uk-council-for-Internet-safety

CEOP:

www.ceop.police.uk/safety-centre/

Childnet:

http://www.childnet.com/

UK Safer Internet Centre:

www.saferInternet.org.uk/safer-Internet-day

www.saferInternet.org.uk/

Internet Watch Foundation:

www.iwf.org.uk

www.iwf.org.uk/members/get-involved

Links to training:

Online Support: online refresher training www.onlinesupport.com/online_training

Movies and presentations:

www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware

Other publications:

- Safer children in a digital world: the report of the Byron Review (PP/D16(7578)/03/08), DCSF and DCMS, 2008; http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/byronreview/.
- Ofcom's response to the Byron Review, Ofcom, 2008; http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/byron/.