Making a Difference
Phoenix Park Academy

Sevenhills
ACADEMY

Online Safety Policy

September 2022

Issue No: 5
Issue Date: Sept 2022
Review Date: Sept 2023
Author: Rachel Patchett
Staff Responsible: R. Patchett
Approved by Governors: October 2022

WELLSPRING
We Make A Difference

What is this policy?

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with ‘Keeping Children Safe in Education’ 2022 (KCSIE) and other statutory documents; it is designed to sit alongside our school’s statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school’s safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. The policy provides guidance for staff, pupils, governors, visitors and parents. Any changes to this policy will be immediately disseminated to all the above stakeholders.

Who is in charge of online safety?

Rachel Patchett is the online-safety coordinator in school and also the Senior Designated Safeguarding lead (DSL). KCSIE makes clear that “the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).”

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 4 Cs: **Content, Contact , Conduct & Commence.** . These four areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all four .

How will this policy be communicated?

This policy is accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Available in paper format in the master policy file located in the Head of Centres office.
- Part of the school induction process for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in annual refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).

AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review

Overview

Aims

This policy aims to:

- Set out expectations for all the staff members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
- for the protection and benefit of the children and young people in their care, and
- for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
- for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Further Help and Support

Internal academy channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with the school's Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH/ Integrated Front Door) and the headteacher will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations we work with may also have advisors to offer general support.

Beyond this, support is available from the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents and anonymous support for children and young people.

Scope

This policy applies to all staff of the Phoenix Park and Sevenhills Academies (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

Roles and responsibilities

Our Academies and all staff members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Staff training - KCSiE 2022

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online safety, that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach. All staff are required to complete annual Online Safety training on National College.

Executive Principal – Mr Phil Hutchinson

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory DfE requirements

Designated Safeguarding Lead / Online Safety Lead – Miss Rachel Patchett/ Mr Phil Burns

Key responsibilities (remember the DSL can delegate certain online-safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Ensure there is regular review and open communication between the DSL's and that clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers school to protect and educate the whole school in their use of technology and establishes mechanisms to identify intervene in and escalate any incident where appropriate."
- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated online safety governor to discuss and monitor online safety in school
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with governors.
- Ensure the 2018 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children Annex A
    - it would also be advisable for all staff to be aware of Part 2 (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation

Governing Body, led by Safeguarding Link Governor

Key responsibilities (quotes are taken from Keeping Children Safe in Education):

- Approve this policy and strategy and subsequently review its effectiveness.
- Ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of DSL [with] lead responsibility for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Ensure that there is regular review and open communication between the DSL's and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Part 2 on Online Safety reflects practice in your school
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction [and] regularly updated in line with advice from the LSCB.
- Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety. Schools should consider this as part of providing a broad and balanced curriculum.

This may include covering relevant issues for schools through Relationships Education (for all primary pupils) and Relationships and Sex Education (for all secondary pupils) and Health Education (for all pupils in state-funded schools) which will be compulsory from September 2020. Schools have flexibility to decide how they discharge their duties effectively within the first year of compulsory teaching and are encouraged to take a phased approach (if needed) when introducing these subjects. The statutory guidance can be found here: Statutory guidance: relationships education relationships and sex education (RSE) and health education. Colleges may cover relevant issues through tutorials. The following resources may help schools and colleges:

- DfE advice for schools: teaching online safety in schools
- UK Council for Internet Safety (UKCIS) guidance: Education for a connected world
- National Crime Agency's CEOP education programme: Thinkuknow
- Public Health England: Rise Above

Governing bodies and proprietors should ensure that online safety is specifically covered within the curriculum. The responsibility for teaching children about online safety is not the sole responsibility of the computing curriculum; it should also be explicitly taught within RSHE and be woven throughout the curriculum for all age groups. One-off events, lessons or assemblies or a reliance on external speakers, are not effective or adequate practice. External speakers can be useful as a catalyst to a discussion or to reinforce learning but are unlikely to be successful if they are the sole source of education or sanctions; in some cases, this approach can undermine settings ability to develop internal capacity to respond to concerns. UKCIS have published guidance for educational settings regarding the use of external visitors.

The SWGfL have produced Project Evolve which aims to provide education resources in line with the strands identified within Education for a connected world.

The online safety curriculum should be flexible, relevant and engage learners' interests, be

- Appropriate to their own needs and abilities and encourage them to develop resilience to online risks.
- Settings should ensure they use a range of relevant resources and be mindful that online safety educate content can date quickly due to the rapid pace of change within technology.
- Good practice is to gain learner input into the online safety curriculum; this could involve use of learner councils or use of peer education approaches

  Governing bodies and   should be aware of 'appropriate filtering and monitoring' as Outlined in KCSiE 2022.

  KCSIE has added a link to harmful online guidance - this includes advice on preparing for any online challenges, hoaxes, sharing information with parents and carers and where to get help and support. Please refer to KCSiE 2022.

Inspection:

As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place. Additional information to support governing bodies and proprietors keep their children safe online (including when they are online at home) is provided in KCSiE 2022.

All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job.
- Know who the Designated Safeguarding Lead's (DSL's) are: Rachel Patchett, Parice Smith, Phil Burns, Jo Indian, Theresa Matthews, Kelly Spence , Kayleigh Johnson , Jackie Chapman, Bev Nalder & Danielle Sparkes. On Line Safety Leads (OSL) – Rachel Patchett and Phil Burns
- Read Part 1 & 2, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- **Sign and follow the staff acceptable use policy**
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum.
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)

- To carefully supervise and guide pupils when engaged in learning activities involving online technology
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues.
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- To to reinforce the importance of school speaking with parents and carers about access to online sites when outside of school.

PHSE Leads -

- Key responsibilities from KCSiE

Teach mental wellbeing, healthy relationships and staying safe online into the PSHE / RE / RSE curriculum, "complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds."

- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE.

Content will include -

- Consent
- Choices
- CSE / CCE
- Unhealthy / abusive family relationships
- Internet/online safety – a much enlarged curriculum theme
- Abusive intimate relationships Refer to RSE Policy

https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education

Guidance for teaching on-line safety in schools:
https://www.gov.uk/government/publications/teaching-online-safety-in-schools

Computing Curriculum Lead – Mr Phil Burns

Key responsibilities:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

All Subject leaders

Key responsibilities:

- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

Network Manager/technician

Key responsibilities:

- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

Data Protection Officer (DPO)

Key responsibilities:

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (April 2018), especially this quote from the latter document:
- GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need.

Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place. Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding

- The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'
- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Pupils

Key responsibilities:

- Listen to, understand, sign and adhere to the pupil acceptable use policy and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- NB: the LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety (but only half talk about it with them more than once a year).
- To engage in discussions with the school regarding online safety .

External groups including parent associations

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

Education and curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE
- Health Education, Relationships Education
- Computing
- Citizenship

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).

At Phoenix Park and Sevenhills academies we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE, and Citizenship. General concerns must be handled in the same way as any other safeguarding concern.

School procedures for dealing with online-safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Acceptable Use Policies

- Data Protection Policy, agreements and privacy statements.

Our academies commit to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also follow procedures outlined in the Whistleblowing Policy.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting; see section below).

Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying.

Sexual violence and harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow appropriate procedure. Staff should work to foster a zero-tolerance culture. Schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). These are defined in the Acceptable Use Policy as well as in this document.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

The school recognises that children and young people are able to access internet and social media via 3G and 4G from personal devices. In an effort to prepare pupils for everyday life, the school will not enforce a blanket ban on this type of technology but instead will assess the age appropriate nature of this type of access and consider supervision needs on an individual basis. The school will continue to educate all pupils in terms of their roles and responsibilities in keeping themselves safe online as well as where to seek help, advice and support.

Social media incidents

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of staff, the academies will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and data security

This section serves to highlight general principles regarding the relationship between safeguarding and data protection / data security.

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

The headteacher/principal, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data- protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At this school we have a secure web connection that is protected with firewalls and multiple layers of security. This is overseen by our IT technician.

Email

- Staff at this school use Google Mail for all school emails. Email accounts are password protected

General principles for email use are as follows:

- Email is the only means of electronic communication to be used between staff and parents (in both directions). Use of a different platform must be approved in advance by the headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Pupils and staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

Academy website

The academy website is a key public-facing information portal for the academy.

Where other staff submit information for the website, they are asked to remember:

- School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published. Parental consent must be given. (Remember also not to save images with a filename that includes a pupil's full name).

Cloud platforms

Cloud platforms used by staff are password protected.

The data protection officer and network manager analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. Parental permission is sought
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At the academies, no member of staff will ever use their personal phone to capture photos or videos of pupils. Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing.

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are taught to be very careful about placing any personal photos on social media. 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 that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Staff, pupils' and parents'

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

Online safety lessons will look at online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Pupils/students are not allowed* to be ‘friends’ with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from ‘following’ staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

Device usage

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

POLICY WRITTEN: September 2022 - R Patchett

REVIEW DATE: September 2023