GREENHEART
LEARNING PARTNERSHIP

E-Safety Policy

2024/2025 Policy Update

Following significant changes to the GLP Governance Framework, all policies are curently under review. Where the existing policies reference local governors or GLAC members, these actions will be undertaken by Partnership Trustees.

Signed off by Trust Board meeting dated: July 2024

Effective from: Original Policy states September 2024

Review Date: Original Policy states July 2025

Contents

1. Aims

This policy applies to all members of the Greenheart community (including GLAC members, staff, volunteers, pupils, parents/carers, visitors) who have access to and are users of academy / Partnership ICT equipment and systems inside or outside of academy buildings.

Our aims are to:

Have robust processes in place to ensure the online safety of members of the Greenheart community.

Deliver an effective approach to online safety, which empowers us to protect and educate the whole community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

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

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying
- Cyber-bullying: advice for Headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and Responsibilities

The Greenheart Local Advisory Committee (GLAC)

The GLAC has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The GLAC members will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

GLAC members will receive a report termly to include an update on e-safety and should include at least the following:

- Monitoring and filtering systems
- Inappropriate usage reports
- Number and occurrences of inappropriate searches and actions thereafter
- An inappropriate search audit
- E-safety training conducted for staff and pupils

The Safeguarding GLAC member will oversee online safety as part of their remit and they are trained to do this.

All GLAC members will:

Ensure that they have read and understand this policy.

Agree and adhere to the Academy ICT & Internet Acceptable Use Policy.

Ensure that online safety is a running and interrelated theme while devising and implementing their approach to safeguarding and related policies and/or procedures.

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The Headteacher

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

The Designated Safeguarding Lead

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the academy child protection policy
- Ensuring that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy behaviour policy
- Updating and delivering staff training on online safety (Appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety to the Headteacher and/or GLAC

This list is not intended to be exhaustive.

The ICT technical team

The ICT technical team is responsible for:

- The ICT technical infrastructure is secure and is protected from misuse or malicious practise
- That there are enforced password structures in place for networks and devices and that passwords are changed regularly
- They remain up to date with guidance regarding their e-safety role and technical updates ensuring these are then shared accordingly to the relevant personnel
- The use of the network, remote access, e mail for misuse, internet and the attempted misuse is monitored, and any breaches are reported to the DSL/E safety co-ordinator (or in the case of teachers reported to the Headteacher) for immediate investigation
- Advice is provided in relation to appropriate software and systems and the monitoring of and updates as per policy
- Any devices including USB sticks, mobile phones, tablets and user areas and accounts are cleared/deleted when staff or pupils leave
- Any ICT equipment no longer fit for purpose is exposed of appropriately and data protection compliant.

This list is not intended to be exhaustive.

All staff and volunteers

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

- They have completed any e-safety training as determined necessary
- They have read and signed the e-safety policy, and have received, acknowledged and use the Academy ICT & Internet Acceptable Use Policy
- They are aware of the reporting system should they have concerns regarding a colleagues inappropriate use of the systems or equipment (whistleblowing)
- They inform the DSL immediately of any concerns regarding a staff or pupil's use of equipment, structures or practises that could cause a pupil harm or others, through the reporting a pupil concern structures
- They remind pupils at given opportunities of the Academy ICT & Internet Acceptable Use Policy to ensure a clear understanding of why this is in place and to support an e-safety ethos
- They act professionally when using the ICT structures and resources are appropriate
- They follow the Data Protection regulations and report any data breaches to the Headteacher
- They ensure that their personal social media is protected through a password and that their behaviours online are appropriate and do not bring disregard to the academy;
- They do not accept social media requests from pupils through networks or e mail, ensuring a professional distance between staff and pupils. They report any such requests to the DSL
- They do not make reference to or have an online discussion regarding an academy, pupils or any other member of the Greenheart community on their social media activities
- They observe parental permissions relating to photographs or videos of pupils and that these are stored appropriately and safely and that they are not duplicated
- Pupils are not expected to use a personal device during the academy day. Where pupils bring personal devices to an academy it is expected that parental permission would be provided and that devices are stored safely by the academy at the start of the day and collected as the pupil leaves
- They do not disclose their passwords to anyone and that passwords are updated regularly
- They do not attempt to bypass any security in place on the computers or devices
- They follow the guidance around copyright material; they do not reproduce materials without the permission of the copyright holder

Parents/Carers

Parents/carers have an essential role in ensuring that their children keep themselves and others safe when using internet/devices, and are encouraged to support the academy in securing good e-safety practice. The academy will inform parents of advice and guidance through a range of networks to ensure they are aware of good e-safety practice. Parents are requested to further support the academy by:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Monitoring their child's use of media and the internet ensuring appropriate filters are age related
- Speaking to their child and ensure that their accounts are password protected and that their child does not publicise their personal details
- Informing the academy of any concerns they have regarding their own child's or other members within the academy community internet or social media usage, these concerns should be passed to the academy safeguarding team
- Having regard for the ICT equipment and resources provided to their child by the academy
- Being mindful not to publish on social media digital and video images taken within the academy at events or performances that have other pupils/staff within the footage due to data protection
- Respecting the academy's Behaviour policy regarding their child's personal devices within the academy

Parents can seek further guidance on keeping children safe online from the following organisations:

- UK Safer Internet Centre
- Childnet International

Pupils

Pupils are responsible for the following:

- They respect the ICT equipment and infrastructure
- They read and follow the Academy ICT & Internet Acceptable Use Policy.
- They respect and follow the academy Behaviour policy regarding their personal devices within the academy setting as set out above
- They understand the rules and consequences of plagiarism and uphold copyright rules
- They respond positively to e-safety lessons, and understand the importance of staying safe on-line
- They understand the importance of reporting abuse, misuse or inappropriate materials and know-how and to whom it should be reported

- They understand the impact cyber-bullying can have on others, they should be thoughtful how they use social media to ensure cyber-bullying is not a concern within the academy
- They respect the use of mobile devices. When pupils are permitted to have their personal devices in academy , pupils must not take images during the academy day or outside of academy which would cause any member of the academy community to feel unsafe or cause disregard to the academy in the wider arena
- They understand the importance good e-safety practice has outside of the academy. All pupils will adhere to the e-safety policy outside of the academy and understand that any breaches relating to themselves or another academy member will have the same consequences as within the academy
- They respect pupil and staff accounts within the academy and do not attempt to or access another's account
- They only use the academy ICT facilities and internet for learning, inappropriate use for example gaming, chat networks could lead to their account being suspended
- They understand that other devices should be used appropriately and in line with e-safety policy and practice

Visitors and members of the community

Visitors and members of the community who use the academy's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use. In some circumstances the academy holds the right to access materials that are being shown to pupils to ensure that the materials are appropriate as per the E-Safety Policy.

4. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum:

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- By the end of primary school, pupils will know
- That people sometimes behave differently online, including by pretending to be someone they are not

- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The safe use of social media and the internet will also be covered in other subjects where relevant

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating Parents about Online Safety

The academy will raise parents' awareness of internet safety in letters or other communications home, and in information via its website and/or newsletters. This policy will also be shared with parents.

The academy will let parents know:

- What systems the academy uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the academy (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Cyber-Bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the Behaviour Policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, GLAC members and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The Academy will also send information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the academy Behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Sexting

This should be read in conjunction with the Child Protection and Safeguarding Policy, Anti-Bullying Policy and Behaviour policy.

For the purpose of this policy, the NSPCC definition and information has been used.

Sexting is the exchange of sexual messages or self-generated sexual images or videos through a mobile phone network or the internet.

Once a message or image has been shared, the sender has no control about how it is used. Sexting can leave a child vulnerable to bullying, blackmail, online grooming or abuse. It is also a criminal offence to create or share explicit images of a child, even if the person doing it is a child.

If a pupil discloses to a staff member that they have been involved with sexting, they should inform the DSL as a matter of urgency who will find out the following:

- If it is an image, video or message
- How the pupil is feeling
- How widely has the image been shared and with whom
- If there were any adults involved
- If the image/video/message is on an organisational or personal device

Staff will not view the image, video or message. If it is on a device belonging to the academy, action should be taken to isolate it. This may involve blocking the network to all users. The DSL will then decide on the best cause of action as per the Child Protection and Safeguarding Policy to ensure the pupil is safe.

Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the academy rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the academy or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Headteacher decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The Behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the academy complaints procedure.

Advice for removing explicit images on the Internet

The Headteacher/DSL in conversations with external services, Police and Social Care will determine when the image can be removed. This may involve:

- Reporting the image to the site or network hosting it
- Contacting the Internet Watch Foundation (IWF)
- Asking the pupil to contact Childline

7. Acceptable use of the Internet in Academies

All pupils, parents, staff, volunteers and GLAC members are expected to sign an agreement regarding the acceptable use of the academy's ICT systems and the internet. Visitors will be expected to read and agree to the academy's terms on acceptable use if relevant.

Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

8. Staff using Devices outside the Academy

For staff using work devices or any device to access work systems, will take appropriate steps to ensure devices and data remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the Academy ICT & Internet Acceptable Use Policy.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT team.

9. How the Academies will respond to issues of Misuse

When incidents of misuse occur, it is essential they are dealt with correctly following the policy as soon as the misuse is suspected or recognised. The academy will clearly define what is classed as inappropriate behaviour in the Academy ICT & Internet Acceptable Use Policy, ensuring all pupils and staff members are aware of what behaviour is expected of them.

Misuse by pupils

- Teachers and other appropriate academy staff have the power to discipline pupils who engage in misbehaviour with regards to internet use, as per the Behaviour Policy
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the DSL/Headteacher
- Pupils who do not adhere to the Academy ICT & Internet Acceptable Use Policy will be sanctioned according to the Behaviour Policy
- Misuse of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with the Child Protection and Safeguarding Policy

- Full access may be withdrawn at any point

Misuse by staff

- Any misuse of the academy's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct by a member of staff should be immediately reported to the Headteacher
- The Headteacher will deal with such incidents in accordance with the academy policy and procedures and may decide to take disciplinary action against the member of staff
- The Headteacher will decide whether it is appropriate to notify the police or the Local Designated Officer (LADO) in their LA of the action taken against a member of staff or for further advice

Use of illegal material

In the event that illegal material is found on the academy's network, or evidence suggest that illegal material has been accessed, the police will be contacted by the Headteacher.

If content being reviewed includes the instances reported below, the investigation should be halted with the Police and LADO informed immediately and the computer/materials isolated and held securely:

- Images of child abuse
- Incidents of grooming behaviour
- Sending obscene materials to a child
- Adult obscene material
- Racist, or criminal material
- Another conduct which could be classed as criminal

10. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages

- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL [and deputy/deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

GLAC members will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the ELT. At every review, the policy will be shared with the GLAC. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

12. Links with other Policies

This online Safety Policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Disciplinary procedures
- Data Protection Policy and privacy notices

- Complaints procedure
- Academy ICT & Internet Acceptable Use Policy