




## Perry Hall Multi-Academy Trust

# ONLINE SAFETY AND ICT ACCEPTABLE USE POLICY

|                              |  |
|------------------------------|--|
| <b>Title</b>                 | PHMAT Online Safety and ICT Acceptable Use Policy                                    |
| <b>Author</b>                | Amarjit Cheema (Trust CEO)   |
| <b>Date Approved</b>         | 27 <sup>th</sup> November 2023   |
| <b>Approved By Name</b>      | Andrew Brocklehurst (Chair of Trustees)  |
| <b>Signature of Approval</b> |  |
| <b>Next Review Date</b>      | November 2025  |

*This policy has been fully consulted on with the following trade unions NAHT, ASCL, NASUWT, Unison, NEU and GMB and was implemented by Perry Hall Multi-Academy Trust (PHMAT) on the above date.*

## PHMAT Online Safety and ICT Acceptable Use Policy

### INDEX

| Section    |   | Page Number |
|------------|---|-------------|
| 1          | Policy Statement  | 3           |
| 2          | Schedule for Development / Monitoring / Review                          | 3           |
| 3          | Scope   | 3           |
| 4          | Role and Responsibilities   | 4           |
| 5          | Education – Pupils  | 6           |
| 6          | Education and Training – Employees / Volunteers                         | 6           |
| 7          | Training - Trustees   | 7           |
| 8          | Technical – infrastructure / equipment, filtering and monitoring        | 7           |
| 9          | Use of Digital and Video Images   | 8           |
| 10         | Using Video Conferencing Facilities with Pupils Such as Microsoft Teams | 9           |
| 11         | GDPR  | 9           |
| 12         | Communications  | 10          |
| 13         | Social Media – Protecting Professional Identity                         | 11          |
| 14         | Unsuitable / Inappropriate Activities                                   | 11          |
| 15         | Responding to Incidents of Misuse                                       | 12          |
| 16         | Trust Actions and Sanctions   | 15          |
| Appendices |   | Page Number |
| Appendix A | AUP Agreement for Employees and Volunteers                              | 17          |
| Appendix B | Employee Laptop Use Agreement   | 22          |
| Appendix C | AUP Agreement for Trustees  | 24          |

## 1. Policy Statement

- 1.1 Perry Hall Multi-Academy Trust (PHMAT) are committed to adopting policies and procedures to encourage a positive working environment.
- 1.3 PHMAT are responsible for ensuring the effective implementation of this Policy. As part of equality monitoring PHMAT will review and monitor the operation of the Policy on a regular basis and in line with the policy review date, alongside consultation with the recognised trade unions.

Any documentation or evidence collected in conjunction with the application of this policy will be treated as confidential and information will only be shared with parties on a need to know basis.

## 2. Schedule for Development / Monitoring / Review

|   |   |
|---|---|
| The implementation of this IT policy will be monitored by the:  | The Board of Trustees                                 |
| Monitoring will take place at regular intervals:  | Annually  |
| The Governing Body will receive a report on the implementation of the IT policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | Annually  |
| Should serious online safety incidents take place, the following persons should be informed   | Data Protection Officer (DPO)<br>Trustee of the Trust |

## 3. Scope

- 3.1 This procedure applies to all employees of PHMAT (including staff, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. Where the term employee is used throughout the policy this applies to both employees and workers.
- 3.2 The purpose of this policy is to ensure that all use of information and communications technology resources is legal, ethical and consistent with the aims, values and objectives of PHMAT.
- 3.3 ICT resources within the Trust must be properly and efficiently used and are not to be used for any activity relating to fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment including sexual harassment, stalking, privacy violation, pornography, gambling, nor any other illegal activity, including peer to peer file sharing. This is an illustrative but not a comprehensive list.
- 3.4 Where any improper ICT activity is suspected (see paragraph above as examples), the Trust reserves the right for Trust Board or their representatives to examine, use and disclose any data found on any school information network or associated systems. In

accordance with this right, Network Administrators will ensure that full access is available at all times. Trust Board may use data found from such examination in disciplinary action and may pass information as evidence to law enforcement officials.

Copies of all policies and procedures referenced above can be accessed via SharePoint.

## **4. Role and Responsibilities**

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

### **4.1 Trustees**

Trustees are responsible for the approval of the IT Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors of Local Boards receiving regular information about online safety incidents and monitoring reports.

### **4.2 Executive and Senior Leaders:**

- The CEO has a duty of care for ensuring the safety (including online safety) of members of the school community
- The CEO/Executive Headteachers and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The CEO/Executive Headteachers and Senior Leaders are responsible for ensuring that the Online safety Coordinator and other relevant staff, this includes the Designated and Deputy designated Safeguarding Leads, receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The CEO/Executive Headteachers and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

### **4.3 Online Safety (IT) Coordinator and DSL:**

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- arranges training and advice for employees
- liaises with the relevant body
- liaises with school technical staff and the Designated Safeguarding Lead
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online safety (Safeguarding) Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

#### 4.4 Network Manager / Technical staff:

The technical infrastructure and internet access for each school is managed by the Trust's technical support provider. The Trust will ensure that the Trust's technical support provider are committed to ensuring the following responsibilities:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the CEO/Executive Headteacher or Senior Leader; Online safety Coordinator

#### 4.5 Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the Trust's IT policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP) **Appendix A**
- when accessing their work Office 365 account from a personal device, that this is done through their own personal device logon only
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

#### 4.6 Child Protection / Safeguarding Designated Person

Should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate online contact with adults / strangers

- potential or actual incidents of grooming
- online-bullying

## **5. Education – Pupils**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Employees should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

## **6. Education and Training – Employees / Volunteers**

It is essential that all employees receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of formal online safety training will be made available to employees. This will be regularly updated and reinforced. An audit of the online safety training needs of all employees will be carried out regularly. It is expected that some employees will identify online safety as a training need within the performance management process.
- All new employees should receive online safety training as part of their induction programme, ensuring that they fully understand the Trust's ICT Policy.

- The Online safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This IT policy and its updates will be presented to and discussed by all employees in staff / team meetings / INSET days.
- The Online safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.
- Training will cover awareness of possibilities of online sexual abuse and harassment that pupils may face

## **7. Training – Trustees**

Trustees should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / online safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for employees

## **8. Technical – infrastructure / equipment, filtering and monitoring**

- The Trust's technical provider will be responsible for ensuring that the Trust's infrastructure / network is as safe and secure as is reasonably possible. The Trust will ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities. Schools will ensure that policies and procedures approved within this policy are implemented.
- (list of responsibilities as currently shown in this section)
- School technical systems will be managed in ways that ensure that the Trust meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of Trust technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to academy technical systems and devices.
- The Central Team is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users.
- The Trust's technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).

The Trust broadband provider has provided the following statement in relation to the filtering measures it which apply:

*"I can confirm we apply all filtering requirements recommend by the Department of Education (DFE) and implement everything under Prevent on our filtering platform.*

*We do filter against the likes of the filter list as provided by CTIRU (Counter terrorism Referral Unit), and others, to make sure our customers keep safe.”*

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly by a third-party IT Support Company- The Trust's infrastructure and individual workstations are protected by up to date virus software.

Guests are permitted access to onsite wifi but not school/Trust networks and Sharepoint. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

## **9. Use of Digital and Video Images**

The development of digital imaging technologies has created significant benefits to learning, allowing employees instant use of images that they have recorded themselves or downloaded from the internet. However, employees need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, employees should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the GDPR Law). To respect everyone's privacy and in some cases of child protection, these images should not be published / made publicly available on social networking sites.
- Employees and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of employees should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers



## 10. Using Video Conferencing Facilities with Pupils Such as Microsoft Teams

Also see Remote learning Policies for each individual school for information on the Home school Agreement of non-negotiables related to online safety and expectations.

Please consider advice on the links below:

<https://www.cobis.org.uk/blog/distance-learning-safeguarding-and-child-protection-guidelines>

<https://swgfl.org.uk/resources/safe-remote-learning/>

<https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19>

## 11. GDPR

Personal data will be recorded, processed, transferred and made available according to the GDPR Law and in conjunction with the Trust Data Protection Policy.

The Trustees must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the GDPR Law.
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- The Data Protection Officer will ensure all schools within the Trust are compliant with current GDPR law

### **Employees must ensure that they:**

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

## 12. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the Trust currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

| Communication Technologies  | Employees & other adults |                          |  |             |
|---|--------------------------|--------------------------|--|-------------|
|   | Allowed                  | Allowed at certain times | Allowed for selected staff with permission from Head | Not allowed |
| Mobile phones may be brought to school  | ✓                        |                          |  |             |
| Use of mobile phones in lessons   |                          |                          |  | ✓           |
| Use of mobile phones in social time   | ✓                        |                          |  |             |
| Staff taking photos on mobile phones / cameras  |                          |                          | ✓  |             |
| Use of other mobile devices e.g. tablets, gaming devices, IWatches or other video-recording devices | ✓                        |                          |  |             |
| Use of personal email addresses in school, or on school network                                     |                          |                          |  | ✓           |
| Use of school email for personal emails   |                          |                          |  | ✓           |
| Use of messaging apps   |                          |                          |  | ✓           |
| Use of social media   |                          |                          |  | ✓           |
| Use of blogs (the school blogsite)  | ✓                        |                          |  |             |

When using communication technologies the Trust considers the following as good practice:

- The official Trust email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Employees should therefore use only the Trust email service to communicate with others when in school, or on school systems (e.g. by remote access)
- Users must immediately report to the nominated person – in accordance with the Trust policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between employees and pupils or parents / carers (email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications
- Whole class / group email addresses may be used at KS1, while pupils at KS2 may be provided with individual school email addresses for educational use
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with

inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies

- Personal information should not be posted on the school website and only official email addresses should be used to identify employees of PHMAT.

### **13. Social Media - Protecting Professional Identity**

PHMAT have a duty of care to provide a safe learning environment for pupils and all staff. Employees who harass, online-bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the Trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

PHMAT provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, employees and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

All employees should ensure that:

- No reference should be made in social media to pupils, parents / carers or any employee of PHMAT
- 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 Trust or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- They do not accept pupils as 'friends' or contacts within any social networking site. Employees could be placing themselves in a vulnerable position. If any employee has already accepted pupils as 'friends' or contacts, then these must be removed.

PHMAT may use social media for professional purposes with authorisation of the Executive Headteacher/Headteacher/Head of School. This will be checked regularly by the CEO/Executive Headteacher/Headteacher/Head of School to ensure compliance with the Social Media, Data Protection.

### **14. Unsuitable / Inappropriate Activities**

The Trust believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

## User Actions

|   |  | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|--|------------|-----------------------------|--------------------------------|--------------|--------------------------|
| <b>Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:</b> | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978                          |            |                             |                                |              | X                        |
|   | Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.  |            |                             |                                |              | X                        |
|   | Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 |            |                             |                                |              | X                        |
|   | Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986                    |            |                             |                                |              | X                        |
|   | Promotion of extremism or terrorism  |            |                             |                                |              | X                        |
|   | Pornography  |            |                             |                                | X            |                          |
|   | Promotion of any kind of discrimination  |            |                             |                                | X            |                          |
|   | Threatening behaviour, including promotion of physical violence or mental harm   |            |                             |                                | X            |                          |
|   | Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute                        |            |                             |                                | X            |                          |
| Using school systems to run a private business  |  |            |                             | X                              |              |                          |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy  |  |            |                             | X                              |              |                          |
| Infringing copyright  |  |            |                             | X                              |              |                          |
| Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)                    |  |            |                             | X                              |              |                          |
| Creating or propagating computer viruses or other harmful files   |  |            |                             | X                              |              |                          |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet)   |  |            |                             | X                              |              |                          |
| Online gaming (educational)   |  |            |                             | X                              |              |                          |
| Online gaming (non-educational)   |  |            |                             | X                              |              |                          |
| Online gambling   |  |            |                             | X                              |              |                          |
| Online shopping / commerce  |  |            | X                           |                                |              |                          |
| File sharing  |  |            | X                           |                                |              |                          |
| Use of social media   |  |            | X                           |                                |              |                          |
| Use of messaging apps   |  |            |                             | X                              |              |                          |
| Use of video broadcasting e.g. Youtube  |  | X          |                             |                                |              |                          |

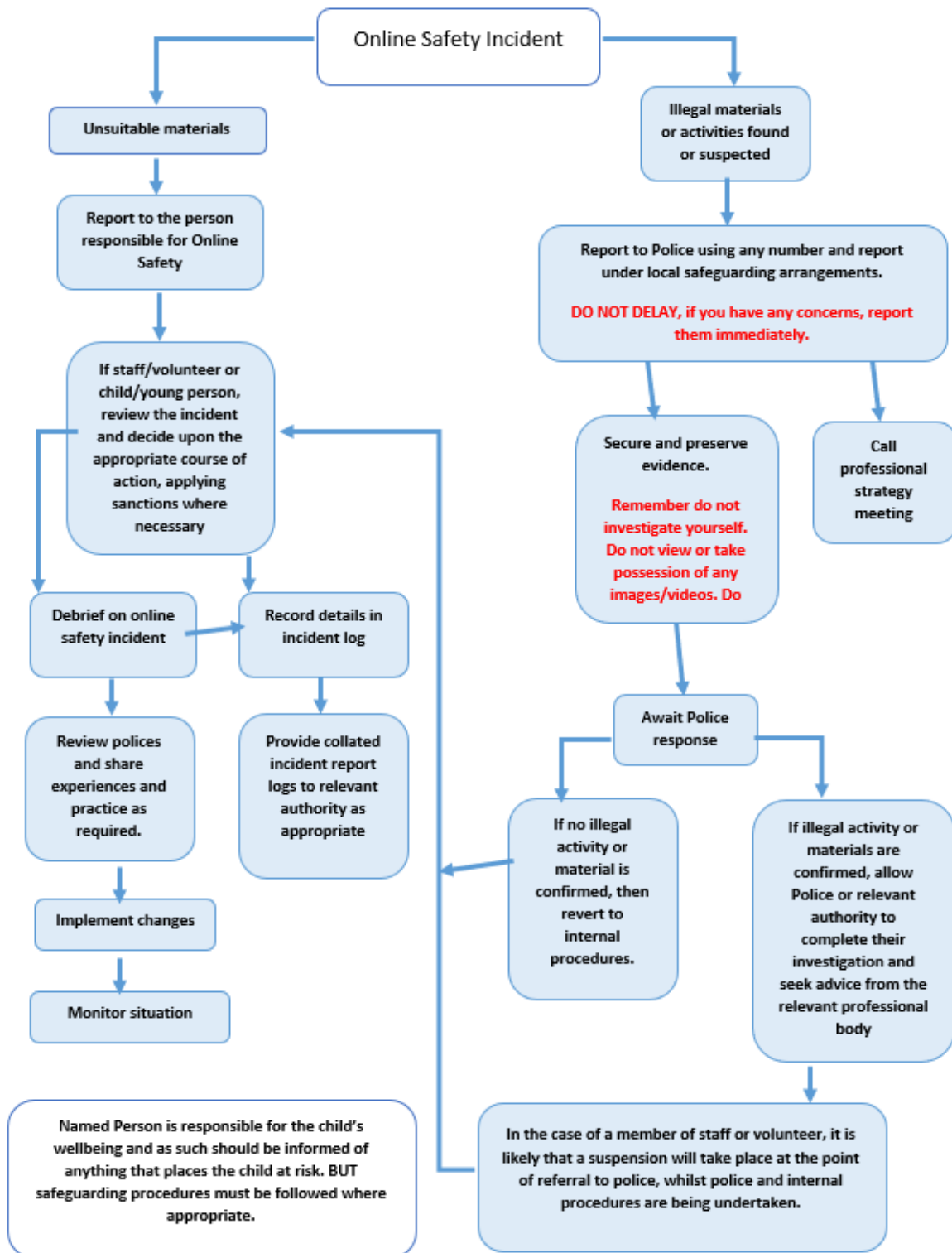
## 15. Responding to Incidents of Misuse

This guidance is intended for use when employees need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities

(see “User Actions” above). Incidents are recorded on CPOMS and reported to the Safeguarding DSL and CEO.

## 15.1 Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



## 15.2 Other Incidents

It is hoped that all employees will be responsible users of digital technologies, who understand and follow the Trust's policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection)
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant)
  - Police involvement and/or action
  - If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
  - Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

It is accepted that it is possible to accidentally access inappropriate material online. If you gain access to a site that would be considered inappropriate by the Trust, or students are seen gaining access to such material, report the URL of the site to the ICT technicians at the earliest opportunity. If in doubt, report.

## **16. Trust Actions and Sanctions**

It is more likely that the Trust will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

## Staff

## Actions / Sanctions

| Incidents:   | Refer to line manager | Refer to Executive Headteacher/<br>Head of School | Refer to Trust HR and LADO | Refer to Police | Refer to Technical Support Staff<br>for action re filtering etc | Warning | Suspension | Disciplinary action |
|--|-----------------------|---|----------------------------|-----------------|---|---------|------------|---------------------|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).       | X                     | X   |                            | X               |   |         | X          | X                   |
| Inappropriate personal use of the internet / social media / personal email   | X                     | X   |                            |                 |   | X       |            |                     |
| Unauthorised downloading or uploading of files   | X                     |   |                            |                 | X   | X       |            |                     |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | X                     | X   |                            |                 | X   | X       |            |                     |
| Careless use of personal data e.g. holding or transferring data in an insecure manner  | X                     | X   |                            |                 |   | X       |            |                     |
| Deliberate actions to breach GDPR Law or network security rules  | X                     | X   | X                          |                 | X   | X       | X          | X                   |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software  | X                     | X   |                            |                 | X   | X       |            | X                   |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature  | X                     | X   | X                          | X               |   |         | X          | X                   |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils                                   | X                     | X   | X                          | X               |   |         | X          | X                   |
| Actions which could compromise the staff member's professional standing  | X                     | X   | X                          | X               |   |         |            | X                   |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school   | X                     | X   |                            |                 |   |         | X          | X                   |
| Using proxy sites or other means to subvert the school's filtering system  | X                     | X   |                            |                 |   | X       | X          |                     |
| Accidentally accessing offensive or pornographic material and failing to report the incident   |                       | X   | X                          |                 |   |         |            |                     |
| Deliberately accessing or trying to access offensive or pornographic material  | X                     | X   | X                          | X               |   |         | X          | X                   |
| Breaching copyright or licensing regulations   |                       | X   |                            |                 |   |         |            | X                   |
| Continued infringements of the above, following previous warnings or sanctions   |                       | X   | X                          |                 |   |         | X          | X                   |





## AUP Agreement for Employees and Volunteers

### Trust Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff employees to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

**This Acceptable Use Policy covers all activities inside and outside of school and is intended to ensure:**

- that employees and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Trust systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.
- the safe use of social media by the Trust its staff, parents, carers and children.

The Trust will try to ensure that employees and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

### Acceptable Use Policy Agreement

*I understand that I must use the Trust's systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.*

### For my professional and personal safety:

- I understand that the Trust will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.

- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Trust.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will make sure that if I use my access my work Office 365 account through a personal device that this will be protected under my own personal device logon.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

**I will be professional in my communications and actions when using Trust ICT systems:**

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with Trust policies and with written consent from the parent, carer or staff member. Images will not be distributed outside of the school network without the permission of the parent/carers or member of staff.
- I will not give out my personal email address or mobile number to any pupils.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the Trust's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

**The Trust has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Schools:**

When I use my mobile devices (laptops / tablets / mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the Trust about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant Trust policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use USB sticks or any external storage devices when in school or in conjunction with my school device.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in Trust policies.
- I will not allow my network user account and password to be used by anyone other than myself, unless required by the Perry Hall Multi Academy Trust.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy Data Protection Policy (or any other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Trust policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that a PIN code, fingerprint or facial recognition is set up when accessing work emails or online systems via my own personal mobile devices.

**When using the internet in my professional capacity or for school sanctioned personal use:**

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

## **I understand that I am responsible for my actions in and out of the school**

- I understand that this Acceptable Use Policy applies not only to my work and use of Trust digital technology equipment in school, but also applies to my use of Trust systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the Trust.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Trustees and in the event of illegal activities the involvement of the police.

## **Social Media**

*As an employee you must:*

- not disclose personal details or identify your geographical location (by disabling access to your geo location to other users), including the publication of photographs where consent has not been given or where it can be reasonably assumed that consent would not be given
- choose online 'friends' carefully – this must NOT include pupils or recent pupils. Remember you cannot guarantee privacy. If you are a teacher in a school and a 'friend' with parents, you must not discuss anything relating to the business of the school and ensure that confidentiality is maintained at all times
- ensure that privacy settings remain unchanged
- not make references to places of work, school, publicise work or private - telephone numbers, addresses or e-mail addresses
- not share private data relating to knowledge obtained through your employment with the Trust
- not disclose any confidential information in relation to your employment
- ensure that online activities do not interfere with your job, your colleagues or commitments to learners and their parents/carers
- ensure that if you identify yourself as a school employee your profile and related content is consistent with how you wish to present yourself with colleagues, learners and their parents/carers.
- not subject your manager or other colleagues to any use of inappropriate or unwanted political or personal reference either in writing, videos, photographs, text messaging, posting blogs, or email that reveal some form of work related behaviour (known as Cyber bullying - to support deliberate and hostile attempts to hurt, upset or embarrass another person). In a case of Cyber bullying, the Senior Leader should refer to PHMAT's Discrimination and Harassment Policy.
- not compromise the Trust by making adverse, damaging or libellous comments, using social media to express views (negative or positive) with which the Trust would not wish to be connected, which are prejudicial to the best interests of the Trust and its employees.
- be careful if using social networking sites to screen employees as you may run the risk of discriminating against candidates

- anyone who identifies themselves as a Trust employee will be required to use a disclaimer on any blogs, for example, stating that “all views are my own and do not necessarily reflect the official position of my employer”
- not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content
- never discuss the school, pupils or parents/carers on social media
- be aware of discussing topics that may be inflammatory

Employees found to be in breach of the Trust’s Social Media policy may be subject to disciplinary action, in accordance with the Local Agreement Disciplinary Procedure for teaching and non-teaching staff in schools, with possible sanctions up to and including dismissal.

Information shared through social media sites, even on private spaces, is subject to copyright, data.

**Managing your personal use of Social Media:**

- “Nothing” on social media is truly private
- Social media can blur the lines between your professional and private life. Do not use the school/Trust logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Employee / Volunteer Name: .....

Signed: .....

Date: .....



## Employee Laptop Use Agreement

### Guidelines for Use

1. The laptop remains the property of Perry Hall Multi Academy Trust
2. The laptop is covered under school insurance, however, the teacher must take reasonable care to avoid damage or loss. The laptop is not covered by school insurance if it is left unattended in a vehicle (this includes being out of site and the boot). All leads and accessories are to be stored safely
3. Teachers are responsible for updating the laptops on a regular basis and ensuring that anti-virus software is kept up to date
4. Internet usage must be of an appropriate nature to minimise pupil's exposure to inappropriate material
5. All laptop faults to be reported to the Trust's ICT technical provider using their reporting procedure
6. The laptop is for the class teacher's usage and must not be transferred to a third party
7. Please make every effort to securely store the laptop and turn off all socket switches at the end of each day

### Terms and Conditions of Use

By signing this 'Laptop Use Agreement Form', I agree to the following terms and conditions of use:

- 1.1. I agree that the laptop at all times remains the property of Perry Hall Multi Academy Trust and that the Laptop is provided for my use as a teacher / support staff employee to assist me in developing educational learning materials for classes taught at Perry Hall Multi Academy Trust.
- 1.2. I undertake to keep the laptop in good working order and to notify of any defect Perry Hall Multi Academy Trust or malfunction of the laptop while in my care.
- 1.3. I will use the laptop lawfully and in accordance with Perry Hall Multi Academy Trust Acceptable Use Policy which may change from time to time, regarding the ethical use of technology, use of legal software, use of the Internet and the protection of personal data.
- 1.4. I will not sell, assign, transfer or otherwise dispose of the laptop.
- 1.5. If my employment status changes with Perry Hall Multi Academy Trust, or if I breach any of these terms or conditions, Perry Hall Multi Academy Trust, may revoke this arrangement by giving me written notice.

1.6. I will take due care of the laptop package at all times, including:

- Not leaving the laptop unattended in a public place.
- Not leaving the laptop unattended or unsecured in a classroom or other place in the school.
- Not leaving the laptop in plain view in an unattended or unsecured vehicle.
- Not allowing the laptop to be accessed by any other person (unless authorized by Perry Hall Multi Academy Trust)
- Not allowing the laptop to be interfered with, tampered with or altered by a third party or otherwise except in prior agreement with Perry Hall Multi Academy Trust.
- Ensuring due care is taken in the handling, transporting and usage of the laptop.

1.7. I will not remove, conceal or alter any laptop package markings, tags or plates or engrave or mark the Laptop in any way that will reduce the value of the laptop.

1.8. If the laptop is lost, stolen or damaged I will advise the Executive Headteacher/Headteacher/ Head of School and the Police as soon as possible.

1.9. I will not allow my network user account and password to be used by anyone other than myself, unless required by the Perry Hall Multi Academy Trust

1.10. I understand that due to current software licensing arrangements covering home use, the laptop package cannot be used by me for any commercial purpose.

**I can confirm that I am willing to accept the responsibility for, taking into my possession a Perry Hall Multi Academy Trust Laptop for the period ..... to .....**

**I confirm that I have read, understood and agree to the above 'Terms and Conditions of Use' and am willing to take responsibility for the laptop subject to these 'Terms and Conditions of Use' and such other policies as are determined by Perry Hall Multi Academy Trust .**

**Laptop make and Serial Number:** \_\_\_\_\_

**Employee name (please print):** \_\_\_\_\_

**Employee signature:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Contact Numbers: Home:** \_\_\_\_\_

**Mobile:** \_\_\_\_\_



## AUP Agreement for Trustees

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to support learning without creating unnecessary risk to users.

### The Trustees will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school, building on Wolverhampton's LA e-Safety Policy and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is understood and not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology (using the Self-Review Framework) to establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

**Name** ..... **Date** .....