Oasis Academy E-Safety Policy Appendix 2017

1. Oasis Academy Henderson Avenue adopts the philosophy, vision and procedures as stated in the E-Safety policy. Clarifying details, minor adjustments and amendments are highlighted in this appendix.
2. Password protection systems have been created and set up by Oasis Central. (Nature of password system page 12 of policy)
3. Legal constraints as defined in the oasis policy.

Academy Strategy for use of Technologies

Whole school planning and procedures for use of technologies

Oasis Academy Henderson Avenue adheres to up to date E- Safety procedures that comply with the Oasis Acceptable Use for Technologies Policy. Responsibility for ensuring that this takes place lies with the Principal (C. Lloyd), Deputy Principal (L. Stroud), SLT members (J. Danson, J. Ashton, L, Brown, J. Sweeting) ICT leaders (C. Cawkwell, H. Gladman) and ICT Technicians (S. Barthwick and A. Mcphee). Ultimately, this is the responsibility of all colleagues in the academy.

The E-safety policy is published on the academy website, E-safety training is provided by the annual Hays online training and periodic updates during the year. Students are reminded of the policy at the beginning of each ICT session. Guidelines and rules are made available to all students on an age appropriate basis. As part of the general safeguarding policy, colleagues and students are aware that any breach of the policy should be reported to the Designated Safeguarding Lead (L. Stroud). From July 2017, breaches would be reported using the CPOMs system.

From the consistent application of central oasis policies, there are clear links from the E-safety policy to other policies including behaviour for learning, curriculum policies and the anti-bullying policy. The sanctions section has been discussed by staff at an Inset and as such are aware of consequences. Any reported incidents or breaches are reported and investigated. Curriculum leaders are aware of the importance of E-Safety within their policies and practices.

Roles and Responsibilities

Oasis Trust Group Executive:

- Has responsibility for ensuring that the E-Safety Policy is implemented across Oasis according to the terms within the policy

- Are responsible for the approval of policies and guidance documents relating to the use of personal learning devices within the Academies
- Has a named individual as the single point of contact for E-Safety issues within Oasis and with National agencies
- Reviews the E-Safety Policy with advice from the National/Regional Oasis Directors, Academy Safeguarding Officers and the Head of Group IT Services

The National/Regional Academy Directors:

- Are responsible for ensuring for reviewing the effectiveness of the policy within an Academy with the Academy Council
- Will receive regular information about E-Safety incidents and monitoring reports for the Academies where they hold responsibility

Oasis Academy Henderson Avenue Principal, Senior Leaders and DSL:
(C. Lloyd, L. Stroud, J. Danson, J. Ashton, L. Brown, J. Sweeting, S. Ward, A. McPhee)

- Are responsible for the day to day implementation of the policies and guidance documents relating to the use of personal learning devices within Oasis
- Will ensure that staff, students and other organisations working with Oasis are aware of the policies and guidance documents
- Will ensure that staff, students, parents/carers all receive suitable opportunities for training in E- Safety. Where a person holds a role with responsibility, they have sufficient knowledge and expertise to carry out their role effectively.
- Will receive regular information about E-Safety incidents and monitoring reports
- Will regularly monitor the effectiveness of the filtering and change control logs
- Will ensure that all staff, external agency personnel, students, parents/carers have completed the relevant Acceptable Use Agreements
- Will ensure that the Incidents and misuse matrices is adhered to by all users.

Oasis National, Regional and site-based IT support teams:

- Will ensure that Oasis infrastructure is secure and is not open to misuse or malicious attack.
- Will ensure that all Oasis-owned student devices will have E-safety software installed. Internet access for any device on the Oasis network is provided through the Oasis filtering system.
- Will ensure that users may only access Oasis's network through an enforced password protection policy in which passwords are required to the agreed IT Managed Service Level Agreement

Use of technologies around the academy.

Acceptable use of technology

Rules for students

These are displayed in all classrooms, ICT suite located on the first floor and communal areas (e.g. Y3/Y4 and Y5/Y6) where group teaching may take place.

□ Keep personal information, password and data safe by ensuring that it is not shared with others.

□ Only access Oasis's network using user account and password,

□ Do not give user name and password to anyone else.

□ If you think someone has learned your password, inform a member of staff immediately.

□ Log off after having finished using the computer.

□ If you find a machine logged on under another user's account, inform a member of staff who will ensure that the machine is safely shut down.

Respect!

□ Show self-respect through your actions. Only use appropriate language and images both within the Learning Platform and on the internet.

□ Do not post inappropriate personal information about your life, experiences or relationships.

□ Do not use any electronic mediums to bully, harass or stalk people.

□ Do not visit any websites that are degrading, pornographic, racist or that Oasis would deem inappropriate

□ Do not abuse access privileges by attempting to or entering other people's private spaces or work areas.

Protect!

□ Ensure that information posted online will put no-one at risk, including you.

□ Do not publish full contact details, a schedule of activities, or inappropriate personal details in public spaces.

□ Report any aggressive or inappropriate behaviour directed at anyone, including you.

□ Do not forward, save or print materials (including emails and images) that Oasis would deem inappropriate or that may cause offence to others.

Oasis Community Learning E-Safety Policy V5.0 December 2016 / IT Services/ Review date: 22

Students are not permitted to bring **Camera phones** into the academy. They are aware of the potential difficulties and dangers of doing so. If a phone camera is brought into school, the teacher or member of the Pastoral team will look after it until the end of the academy day. If the situation is repeated or frequent, parents would be informed and a meeting held. In exceptional circumstances, where a phone is needed for safety/CP/safeguarding issues, an adult would take control of the phone for the day.

Webcams are not used by the students independently and would only be used under strict adult guidance. Peer to Peer networks are not used in the academy.

Incidents and sanctions

In accordance with the OAHA child protection guidelines, the academy has completed a structure for what should/could happen if there are reports of misuse of ICT technology. It provides guidance that users shall not visit internet sites, make posts, download, upload, transfer data, communicate or pass on inappropriate material, remarks, proposals or comments. For completed matrices, please refer to pages 27-31 of the main policy.

A flow diagram for the reporting of incidents can be found on page 32 of the main E-safety policy. For more serious incidents, referral should be made to either the Principal or designated safeguarding Lead in person. This should then be followed up by completing an incident form using the CPOMs system.