HMFA

Herefordshire Marches
Federation of Academies

E-Security Policy

September 2016

Next Review Due: January 2017

Strategic and operational practices

At all HMFA academies and schools:

- Stewart Morehead is the Senior Information Risk Officer (SIRO).
- We will ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.
- The academy or school's Designated Data Controller is the Academy Office Manager or School Business Manager. This person is responsible for ensuring compliance with the Data Protection Act and implementation of this policy.
- Staff must report any concerns about Data Protection or E-Security to the Academy or School Business Manager who will contact Deputy Headteacher (IT), the Technical support company and the school's ICT and Esafety Co-ordinators. Each Academy or school has it's own list of contacts available displayed in the staffroom.
- All staff are DBS checked and records are held in one central record on SIMS.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
    - staff
    - governors (Each academy or school Governor Secretary needs a list of which governors have RD web, SIMS, remote email access to school systems).
    - pupils
    - parents
    - students (the Academy or schools Student Manager should provide a list of students to the Technical Support company and provide start and leaving dates. The Technical Support company will set up a limited access to the school network for students and disable accounts at the end of the placement.

  The Acceptable Use Agreement form clears all responsibilities and expectations with regard to data security.

- We have approved educational web filtering across our wired and wireless networks.
  We researching possible solutions to provide an additional layer of monitoring software across our network system, emails, blogs etc.
- We follow Herefordshire LA guidelines for the transfer of any data, such as SIMs data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- We require staff to use STRONG passwords for access into our MIS system. *A strong password consists of a combination of capital letters, lower case letters, numbers and characters.*
- We require staff to change their passwords into SIMs and the network twice a year. Our Technical support company will force the password change on the 1st October and again on 1st February.
  Duncan - How can we ensure SIMS passwords are changed twice a year?
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school, and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff who set up usernames and passwords for e-mail and network access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical or manual solutions

- Staff have secure areas on the network to store sensitive documents such as Pupil, Personel, Pastoral, SEN, Assessment or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 mins. idle time.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use < RAv3 / VPN solution > with its 2-factor authentication for remote access into our systems.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- We use the Herefordshire LA Admissions system to transfer admissions data.
- Our Technical Support engineers create online user accounts for access to broadband services. We are currently researching automating services for the creation of user accounts.
- We use ANYCOMMS to transfer documents to schools in Herefordshire, such as references, reports of children.
- Lord Scudamore Academy use <name of product/company> for cloud based back up of SIM / SCO Server and the PSF Server. The SQL Database agent and file backups are included. The UK Datacentre complies with Data Protection requirements. It provides a fully encrypted solution.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable area.
- All servers are in lockable locations and managed by DBS-checked staff.
- At Lord Scudamore Academy we lock any back-up tapes in a secure, fire-proof cabinet. Back-ups are encrypted. We are currently ensuring that all of our HMFA Academies and St Weonards Primary School have purchased a secure/fire proof cabinet so that we can ensure that no back-up tapes leave the site on mobile devices To be added to ICT Strategic Plan 2015.
- We use <name here> remote secure back-up / named alternative solution> for disaster recovery on our network / admin, email, curriculum servers.
- We comply with the WEEE directive on equipment disposal. Our technical Support company uses an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.
- Laptops loaned by the school for use by staff at home, where used for any protected data, is disposed of through the same procedure. Staff ipads are exempt from this as they are not used to store sensitive data.
- Paper based sensitive information is shredded, using a cross-cut shredder.
- HMFA academies and schools do not store any parents credit card data. We are developing the use of parents online payment systems within our schools. All credit card information will be stored by the Online payment system. In the case of Lord Scudamore Academy, we use Tucasi/SCOpay which uses the World Pay system. Which complies with Data Protection Act 1998 and is PCI DSS compliant.

Policy created by Jo Brace (Deputy Headteacher (IT) in consultation with all Executive Headteachers, the SIRO, all HMFA Business Managers, HMFA Directors and Academy/School Governors, Lord Scudamore Academy ICT Co-ordinator, HMFA Safeguarding Manager, all HMFA Technical Support companies and the HMFA Bursar

This policy was created based on a template provided by LGfL and SWfL.