Appendix 1 – DCLG 10 Steps to Cyber Security

Cyber Security Measure
Information Risk Management Regime - Assess the risks to your organisation's information assets with the same vigour as you would for legal, regulatory, financial or operational risk. To achieve this, embed an Information Risk Management Regime across your organisation, supported by the Board, senior managers and an empowered information assurance (IA) structure. Consider communicating your risk management policy across your organisation to ensure that employees, contractors and suppliers are aware of your organisation's risk management boundaries.
Secure configuration - Introduce corporate policies and processes to develop secure baseline builds, and manage the configuration and use of your ICT systems. Remove or disable unnecessary functionality from ITC systems, and keep them patched against known vulnerabilities. Failing to do this will expose your business to threats and vulnerabilities, and increase risk to the confidentiality, integrity and availability of systems and information.
Network security - Connecting to untrusted networks (such as the Internet) can expose your organisation to cyber-attacks. Follow recognised network design principles when configuring perimeter and internal network segments, and ensure all network devices are configured to the secure baseline build. Filter all traffic at the network perimeter so that only traffic required to support your business is allowed, and monitor traffic for unusual or malicious incoming and outgoing activity that could indicate an attack (or attempted attack).
Managing user privileges - All users of your ICT systems should only be provided with the user privileges that they need to do their job. Control the number of privileged accounts for roles such as system or database administrators, and ensure this type of account is not used for high risk or day-to-day user activities. Monitor user activity, particularly all access to sensitive information and privileged account actions (such as creating new user accounts, changes to user passwords and deletion of accounts and audit logs).
User education and awareness - Produce user security policies that describe acceptable and secure use of your organisation's ICT systems. These should be formally acknowledged in employment terms and conditions. All users should receive regular training on the cyber risks they face as employees and individuals. Security related roles (such as system administrators, incident management team members and forensic investigators) will require specialist training.

Incident management - Establish an incident response and disaster recovery capability that addresses the full range of incidents that can occur. All incident management plans (including disaster recovery and business continuity) should be regularly tested. Your incident response team may need specialist training across a range of technical and non-technical areas. Report online crimes to the relevant law enforcement agency to help the UK build a clear view of the national threat and deliver an appropriate response.
Malware prevention - Produce policies that directly address the business processes (such as email, web browsing, removable media and personally owned devices) that are vulnerable to malware. Scan for malware across your organisation and protect all host and client machines with antivirus solutions that will actively scan for malware. All information supplied to or from your organisation should be scanned for malicious content.
Monitoring - Establish a monitoring strategy and develop supporting policies, taking into account previous security incidents and attacks, and your organisation's incident management policies. Continuously monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate attacks and the compromise of data. Monitor all ICT systems using Network and Host Intrusion Detection Systems (NIDS/HIDS) and Prevention Systems (NIPS/HIDS).
Removable media controls - Produce removable media policies that control the use of removable media for the import and export of information. Where the use of removable media is unavoidable, limit the types of media that can be used together with the users, systems, and types of information that can be transferred. Scan all media for malware using a standalone media scanner before any data is imported into your organisation's system.
Home and mobile working - Assess the risks to all types of mobile working (including remote working where the device connects to the corporate network infrastructure) and develop appropriate security policies. Train mobile users on the secure use of their mobile devices for locations they will be working from. Apply the secure baseline build to all types of mobile device used. Protect data-at-rest using encryption (if the device supports it) and protect data-in-transit using an appropriately configured Virtual Private Network (VPN).