|  |  |
| --- | --- |
| **Oxford Diocesan Schools Trust**School Effectiveness Service |  |
| Church House Oxford 🞄 Langford Locks🞄 Kidlington 🞄 Oxford 🞄 OX5 1GF |

|  |  |  |  |
| --- | --- | --- | --- |
| Original document | Internal Officer Scrutiny | V1 draft | 25/8/17 |
| Amended  | Trust Consultation | V1.1 Draft |  |
| Amended | Curriculum & Ethos Committee | V1.2 Draft |  |
| FINAL document | Full Board (adopted) | FINAL | 17/10/17 |

|  |  |
| --- | --- |
| 5 | ODST Non-Statutory Document or Framework (a document produced to support leaders and governors for their consideration as guidance or support for routines and activities in various areas of the school.)  |

**School Technical Security Guidance (including filtering and passwords)**

1. **Introduction**
	1. Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The relevant body has chosen to delegate its functions to local governing bodies and headteachers and the local governing body are responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:
* users can only access data to which they have right of access
* no user should be able to access another’s files (other than that allowed for monitoring purposes within the school’s policies).
* access to personal data is securely controlled in line with the school’s personal data policy
* logs are maintained of access by users and of their actions while users of the system
* there is effective guidance and training for users
* there are regular reviews and audits of the safety and security of school computer systems
* there is oversight from senior leaders and these have impact on policy and practice.
	1. If the schoolhas a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that might otherwise be carried out by the schoolitself (as suggested below). It is also important that the managed service provider is fully aware of the schoolOnline Safety Policy / Acceptable Use Agreements). The schoolshould also check guidance on these technical issues.
1. **Responsibilities**
	1. Trustees would urge that the management of technical security in ODST schools is clearly set down as the responsibility of a senior member of staff. (schools may choose the Network Manager / Technical Staff / Head of IT or another relevant responsible person).
2. **Technical Security** **Policy guidance**
	1. ODST schools are responsible for ensuring that their infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved by the local governing body are implemented. They will also need to ensure that the relevant people receive guidance and training and are effective in carrying out their responsibilities. Schools will have very different technical infrastructures and differing views as to how these technical issues are handled – it is therefore essential that this section is fully discussed by a wide range of staff – technical, educational and administrative staff before these statements are agreed and added to the policy.
	2. Technical Security Checklist – schools and governors should audit their network and IT security regularly and the following checklist is the trust’s recommended process for reporting back on the robustness of systems and procedures.

| **Checklist** | In Place | Partially | Not in Place |
| --- | --- | --- | --- |
| School technical systems are managed in ways that ensure that the school meets recommended technical requirements as outlined in the trust’s online safety policy and guidance. |  |  |  |
| There are regular reviews and audits of the safety and security of school technical systems |  |  |  |
| Servers, wireless systems and cabling are securely located and physical access restricted. |  |  |  |
| Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. |  |  |  |
| Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (schools may wish to provide more detail).  |  |  |  |
| All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users are recorded by the Network Manager / Technical Staff (or other person) and are reviewed, at least annually, by the local governing body (LGB). |  |  |  |
| Users are taught about and made responsible for the security of their username and password and do allow other users to access the systems using their log on details. They know what to do if there has been a breach of security. |  |  |  |
| A named member of staff 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 |  |  |  |
| Mobile device security and management procedures are in place for school provided devices and / or where mobile devices are allowed access to school systems.  |  |  |  |
| School leaders/staff 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 technical incident to the Network Manager / IT Leader. |  |  |  |
| An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school system. |  |  |  |
| An agreed policy is in place regarding installation of programmes on school devices by users |  |  |  |
| An agreed policy is in place (to be described) regarding the type of use on school devices that may be used out of school.  |  |  |  |
| An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices |  |  |  |
| The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc |  |  |  |
| Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured |  |  |  |

1. **Password Security**
	1. A safe and secure username / password system is essential if network security is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE). Where sensitive data is in use – particularly when accessed on laptops / tablets – schools should use more secure forms of authentication. Where this is adopted, trustees expect the policy to state clearly that items such as hardware tokens must be stored separately from the laptop when in transit – to avoid both being lost / stolen together.
	2. Trustees are clear that our Primary schools will need to decide at which point they will allocate individual usernames and passwords to pupils. They may choose to use class log-ins for KS1 (though increasingly children are using their own passwords to access programmes). ODST Schoolsneed to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the acceptable user policy. Trustees would urge schools to consider the implications of using whole class log-ons when providing access to learning environments and applications, which may be used outside school.
	3. Password Security Checklist

| **Checklist** | In Place | Partially | Not in Place |
| --- | --- | --- | --- |
| All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users are recorded by (named individual) (or other person) and are reviewed, at least annually, by the LGB (or other group).  |  |  |  |
| All school networks and systems are protected by secure passwords that are regularly changed  |  |  |  |
| The “master / administrator” passwords for the school systems, used by the technical staff is available to the Headteacher or other nominated senior leader and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts. (A school should never allow one user to have sole administrator access) |  |  |  |
| All users (adults and where issued, pupils) have responsibility for the security of their username and password know they must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. |  |  |  |
| Passwords for new users, and replacement passwords for existing users are allocated by a named member of staff |  |  |  |
| **Staff Passwords** |  |  |  |
| All staff users are provided with a username and password by a named member of staff / automated process) who / which will keep an up to date record of users and their usernames. |  |  |  |
| Staff passwords are changed regularly  |  |  |  |
| **Pupil Passwords (where issued)** |  |  |  |
| All users (at KS2 and above) are provided with a username and password by a named member of staff who will keep an up to date record of users and their usernames |  |  |  |
| Users are required to change their password every (insert period).  |  |  |  |
| Students / pupils are taught the importance of password security |  |  |  |

* 1. It is essential that users are made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ins are being used.
	2. Members of staff should be made aware of the school’s password policy:
* at induction
* through the school’s online safety policy and password security policy
* through the Acceptable Use Agreement
	1. Pupils should be made aware of the school’s password policy:
* in lessons (schools should describe how this will take place)
* through the Acceptable Use Agreement

1. **Filtering**

36

* 1. The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. Trustees expect internet access to be filtered for all users. Differentiated internet access should be available for staff and customised filtering changes managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system.
	2. Where personal mobile devices are allowed, internet access through the school network, should ensure that filtering is applied that is consistent with school practice.
	3. Filtering Checklist

| **Checklist** | In Place | Partially | Not in Place |
| --- | --- | --- | --- |
| The school maintains and supports the managed filtering service provided by the Internet Service Provider**Or**The school manages an alternative filtering service and the LGB/Headteacher is able to show, in the event of any legal issue, that the school meets its statutory requirements to ensure the safety of staff, pupils and other users. |  |  |  |
| The school provides differentiated user-level filtering through the use of the (insert name) filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff, pupils etc.) |  |  |  |
| In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this is logged and carried out by a process that is agreed by the Headteacher |  |  |  |
| Mobile devices that access the school internet connection (whether school or personal devices) are subject to the same filtering standards as other devices on the school systems |  |  |  |
| Any filtering issues are reported immediately to the filtering provider |  |  |  |
| Requests from staff for sites to be removed from the filtered list are considered by (insert name or title) (nb an additional person should be nominated – to ensure protection for the Network Manager or any other member of staff, should any issues arise re unfiltered access). If the request is agreed, this action is recorded and logs of such actions are reviewed regularly by the LGB.  |  |  |  |
| Pupils made aware of the importance of filtering systems through the online safety education programme (schools may wish to add details). They will also be warned of the consequences of attempting to subvert the filtering system. |  |  |  |
| Staff users are made aware of the filtering systems through: (amend as relevant) * the Acceptable Use Agreement
* induction training
* staff meetings, briefings, Inset.
 |  |  |  |
| Parents are informed of the school’s filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc. (amend as relevant) |  |  |  |

1. **Monitoring**
	1. ODST recognises that no filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. Trustees would urge leaders to report this to governors at least annually and a record of internet access and breaches of the schools filtering mechanisms included in headteacher reports.
2. **Audit / Reporting**
	1. Logs of filtering change controls and of filtering incidents must be made available to:
* The headteacher
* the second named responsible person for internet security
* A named E-Safety Governor or governor’s committee
* External Filtering provider / ODST officers
	1. Logs of filtering incidents are now a feature of Ofsted inspections and so ODST would expect all its schools to be able to provide and discuss this feature of the school’s child protection and safeguarding culture. Logs are also required by local authority designated officer (LADO) and the Police on request, when investigating serious safeguarding incidents.
	2. The filtering policy is reviewed in response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary).
1. **Further Guidance**

35

* 1. Our schools may wish to seek further guidance. The following is recommended:
* Schools in England (and Wales) are required *“to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"*([Revised Prevent Duty Guidance: for England and Wales, 2015](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf)).
* UKSIC produced guidance on / information on “[Appropriate Filtering](http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-for-education-settings)”
* NEN Technical guidance: <http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/>